Bond Law Review

Volume 19 | Issue 1 Article 7

2007

Protecting Privacy on the 'Borderless' Internet - Some Thoughts on Extraterritoriality and Transborder Data Flow

Dan Jerker B. Svantesson
Bond University, dan_svantesson@bond.edu.au

Protecting Privacy on the 'Borderless' Internet - Some Thoughts on Extraterritoriality and Transborder Data Flow

Abstract
Extract Providing adequate protection of privacy is not easy in a society dominated by highly developed technologies. A large portion of our communications takes place over an open network – the Internet – designed without privacy in mind. Our browsing habits are tracked by various technologies such as so-called cookies, and the terms we use to search the World Wide Web (WWW) are logged by search engine providers. The e-mails we send are typically as private as postcards and strong industry organisations are seeking to find out what we download, so as to make sure we are not infringing copyrights.

Keywords
protecting privacy, transborder data flow, borderless internet

PROTECTING PRIVACY ON THE 'BORDERLESS' INTERNET – SOME THOUGHTS ON EXTRATERRITORIALITY AND TRANSBORDER DATA FLOW

DAN JERKER B SVANTESSON*

Providing adequate protection of privacy is not easy in a society dominated by highly developed technologies. A large portion of our communications takes place over an open network – the Internet – designed without privacy in mind. Our browsing habits are tracked by various technologies such as so-called cookies, and the terms we use to search the World Wide Web (WWW) are logged by search engine providers. The e-mails we send are typically as private as postcards and strong industry organisations are seeking to find out what we download, so as to make sure we are not infringing copyrights.

While it, thus, undeniably is difficult to provide adequate privacy protection on a national level, the difficulties are even greater on an international level where the regulator is faced with the additional dimension of the jurisdictional reach of the regulation. Australian privacy law addresses this international dimension in two ways: (1) by giving the *Privacy Act 1988* (Cth) extraterritorial application, and (2) by regulating transborder data flow.

This article examines how the Australian approach to these issues work in relation to the 'borderless' Internet. It highlights some relevant policy considerations, and is aimed at assisting in legal reform, as well as at bringing attention to these issues on a broader scale.

In the context of the extraterritorial application of the *Privacy Act* it gives particular attention to what is meant by and organisation *carrying on business in Australia* and personal information being *collected or held by the organisation in Australia*. These concepts are of crucial importance for the extent of the extraterritorial reach of the Act. Yet, so far they have been the object of little discussion.[1]

* Assistant Professor, Faculty of Law, Bond University, Gold Coast Queensland 4229 Australia.

1 One of the few exceptions being Jon Bing, *Data protection, jurisdiction and the choice of law* [1999] PLPR 65.

Further, as far as the regulation of transborder data flow is concerned, the article emphasises the importance of the consent requirement being given an appropriately strict interpretation, and notes a few changes that could be made to improve the Australian regulation of transborder data flow.

The extraterritorial reach of the Privacy Act

The extraterritorial reach of the *Privacy Act* is regulated in s. 5B. That section extends the application of the *Privacy Act* to acts done, or practice engaged in, outside Australia by an organisation provided that certain requirements are met. Those requirements relate to three separate issues:

1. the legality of the act or practice under the law of the country in which it took place;
2. the nature of the data subject (i.e. the person the personal information relates to); and
3. the nature of the organisation transferring the data.

The first two requirements are rather uncontroversial. In relation to the first requirement, s. 5B states that: 'The act or practice overseas will not breach a National Privacy Principle [NPP[2]] or approved privacy code or be an interference with the privacy of an individual if the act or practice is required by an applicable foreign law.' As far as the second requirement is concerned, s. 5B makes clear that the Act only has extraterritorial effect where the act or practice relates to personal information about an Australian citizen or another person whose continued presence in Australia is not subject to a limitation as to time imposed by law.[3]

The third requirement is more complex, and s. 5B outlines two different scenarios in which this requirement is met. Under s. 5B(2), the requirement is met where the organisation in question is:

- 'an Australian citizen';[4] or
- 'a person whose continued presence in Australia is not subject to a limitation as to time imposed by law'[5]; or
- 'a partnership formed in Australia or an external Territory'[6]; or

---

2 The *Privacy Act 1988* (Cth) contains ten National Privacy Principles that regulate the private sector.

3 *Privacy Act 1988* (Cth), s. 5B(1)(a).

4 *Privacy Act 1988* (Cth), s. 5B(2)(a).

5 *Privacy Act 1988* (Cth), s. 5B(2)(b).

- 'a trust created in Australia or an external Territory'[7]; or
- 'a body corporate incorporated in Australia or an external Territory'[8]; or
- 'an unincorporated association that has its central management and control in Australia or an external Territory.'[9]

Extraterritorial claims based on s. 5B(2) – where the organisation in question falls within one of the categories outlined above – seem rather uncontroversial as the link between Australia and the organisation in question is substantial indeed. Such jurisdictional claims ought to be well within the limits arguably imposed by public international law.[10]

However, the Australian rules go further. Under s. 5B(3) the requirement as to the nature of the organisation transferring the data is met where all of the following conditions are met:

- 'the organisation is not described in subsection (2)'[11];
- 'the organisation carries on business in Australia or an external Territory'[12]; and
- 'the personal information was collected or held by the organisation in Australia or an external Territory, either before or at the time of the act or practice.'[13]

Compared to extraterritorial claims based on s. 5B(2), claims based on s. 5B(3) are arguably not as solidly founded in public international law principles. However, that is not to say that claims under s. 5B(3) are not in line with the principles of public international law. Indeed, as s. 5B(1) limits the application to those situations where there is a clear link between Australia and the data subject, claims under s. 5B(3) would seem to be justifiable with reference to the so-called objective territoriality principle,[14] the passive personality principle[15] or at least the more modern effects doctrine[16].

---

6 *Privacy Act 1988* (Cth), s. 5B(2)(c).

7 *Privacy Act 1988* (Cth), s. 5B(2)(d).

8 *Privacy Act 1988* (Cth), s. 5B(2)(e).

9 *Privacy Act 1988* (Cth), s. 5B(2)(f).

10 'Introductory Comment to the Harvard Draft Convention on Jurisdiction with Respect to Crime 1935' (1935) 29 Supp 443 *American Journal of International Law*, 445.

11 *Privacy Act 1988* (Cth), s. 5B(3)(a).

12 *Privacy Act 1988* (Cth), s. 5B(3)(b).

13 *Privacy Act 1988* (Cth), s. 5B(3)(c).

14 Jurisdiction based on the offending activity, while taking place outside the territory of the forum, having its primary effect within the territory of the forum. See generally: I.

At the same time, it must be acknowledged that the language used in s. 5B(3) does not make it possible to assess the details of its application. To be able to do so, one would need to know exactly what is meant by *carrying on business in Australia*, and under which circumstances it could be said that personal information was collected or held by the organisation *in Australia*.

As affected individuals cannot take civil actions in Australian courts where their privacy is being violated, there are no court decisions to clarify these two issues. Further, at the time of writing there are no reported determinations made by the Privacy Commissioner that provide guidance. Indeed, there are no such determinations at all relating to the extraterritorial application of the Act. Furthermore, as far as the meaning of *carrying on business in Australia* is concerned, only limit guidance can be drawn from how other Acts using that phrase have been applied.

Carrying on business in Australia

The *Corporations Act 2001* (Cth) gives one definition of what it is to "carry on business in Australia". Section 21 of that Act is of particular relevance. In sub-section 1, it makes clear that a body corporate that has a place of business in Australia, carries on business in Australia. This is hardly surprising and adds nothing to our understanding of how to interpret the phrase in the context of the *Privacy Act*. Similarly, sub-section does not add much for our purposes in making clear that a body corporate is carrying on business in Australia where it uses a share transfer office or share registration office in Australia, or is 'administering, managing, or otherwise dealing with, property situated in Australia […], as an agent, legal personal representative or trustee, whether by employees or agents or otherwise'[17]. The interesting part of s. 21 is sub-section 3 which outlines some connecting factors that on their own do not mean that a body corporate is carrying on business in Australia:

Brownlie, *Principles of Public International Law* 5th ed. (Oxford: Oxford University Press, 2001), at 303-306.

15 Sometimes referred to as the passive nationality principle. "According to this principle aliens may be punished for acts abroad harmful to nationals of the forum." I. Brownlie, *Principles of Public International Law* 5th ed. (Oxford: Oxford University Press, 2001), at 306.

16 Jurisdiction based upon the fact that conduct outside the state has effects within the state. See further: D. J. Gerber, 'Beyond Balancing: International Law Restrains on the Reach of National laws' (1984) 10 *Yale Journal of International Law*, 185,190.

17 *Corporations Act 2001* (Cth), s. 21(2)(b).

> [A] body corporate does not carry on business in Australia […] merely because, in Australia […] the body:
>
> (a) is or becomes a party to a proceeding or effects settlement of a proceeding or of a claim or dispute; or
>
> (b) holds meetings of its directors or shareholders or carries on other activities concerning its internal affairs; or
>
> (c) maintains a bank account; or
>
> (d) effects a sale through an independent contractor; or
>
> (e) solicits or procures an order that becomes a binding contract only if the order is accepted outside Australia […]; or
>
> (f) creates evidence of a debt, or creates a charge on property; or
>
> (g) secures or collects any of its debts or enforces its rights in regard to any securities relating to such debts; or
>
> (h) conducts an isolated transaction that is completed within a period of 31 days, not being one of a number of similar transactions repeated from time to time; or
>
> (j) invests any of its funds or holds any property.[18]

At least two comments must be made about how this helps us understand the interpretation of the phrase 'carrying on business' in the context of the Privacy Act. First, due to the different context in which s. 21 of the Corporations Act 2001 (Cth) operates, it is important not to place too much emphasis on what is said in this Act. Second, s. 21 of the Corporations Act 2001 (Cth) does not exclude the possibility that a combination of the activities outlined in sub-section 3 would amount to carrying on business in Australia. Indeed, by using the wording 'a body corporate does not carry on business in Australia […] merely because', the section leaves open the possibility that one such activity, in certain circumstances, could mean that the body corporation engaging in that activity is carrying on business in Australia.

The Civil Procedure Rules of some Australian states also refer to 'carrying on business'. For example, *Uniform Civil Procedure Rules 1999* (Qld) s. 124(g)(ii) allows service to be made outside Australia where the proceeding relates to a contract 'made by 1 or more parties carrying on business or residing in Queensland'. However, no

[18] *Corporations Act 2001* (Cth), s. 21(3).

cases have considered, in detail, the question of what amounts to 'carrying on business', and thus, no assistance can be gained from this area of law.

In *Hope v Bathurst City Council*[19], the phrase 'carrying on business' was considered in the context of whether certain land came within the definition of 'rural land' for the purpose of a Local Government Act. Mason J noted that: "the words 'carrying on' […] imply the repetition of acts […] and activities which possess something of a permanent character."[20] While such an observation may have been appropriate in the context it was made, its value in the privacy context can be questioned. As discussed in more detail below, it is undeniable that severe privacy violations can occur in, or result from, single contacts between the offender and the data subject.

Of the Acts using the phrase carrying on business in Australia, the most relevant is the *Trade Practices Act 1974* (Cth) ('TPA'), which in s. 5(1) also refers to carrying on business. Interestingly, just as the *Privacy Act*, the TPA uses the phrase in the context of outlining the extraterritorial application. Unfortunately, there is no case law to clarify the exact scope of the TPA's use of the phrase. However, some aspects have been clarified through the Federal Court's decision in *Bray v F. Hoffman-La Roche Ltd*[21]:

- Whether or not a body corporate is "carrying on business" is to be assessed at time of contravention;[22]
- Whether or not a body corporate is 'carrying on business' is a question of fact;[23]
- There is no requirement that to 'carrying on business' an organisation need a place of business in Australia;[24]
- Having a branch in Australia is sufficient to be viewed as 'carrying on business' in Australia in some contexts;[25] and
- TPA s. 5(1) does not determine the jurisdictional question. For an action to be taken in an Australian court, that court must be able to claim jurisdiction over the dispute.[26]

---

19 (1980) 144 CLR 1.

20 *Hope v Bathurst City Council* (1980) 144 CLR 1, at 8-9.

21 [2002] FCA 243.

22 *Bray v F. Hoffman-La Roche Ltd* [2002] FCA 243, at para 57.

23 *Bray v F. Hoffman-La Roche Ltd* [2002] FCA 243, at para 62.

24 *Bray v F. Hoffman-La Roche Ltd* [2002] FCA 243, at para 63.

25 *Bray v F. Hoffman-La Roche Ltd* [2002] FCA 243, at 63.

26 *Bray v F. Hoffman-La Roche Ltd* [2002] FCA 243, at para 191.

While it is clear that little guidance can be drawn from the TPA's use of the phrase carrying on business, the question nevertheless arises whether privacy law should take the same approach as the TPA? Doing so is undeniably an attractive option from the perspective of consistency. Further, the conclusions drawn from *Bray v F. Hoffman-La Roche Ltd* seem appropriate also for the privacy context.

Leaving aside decisions by the Privacy Commissioner and the interpretation given in the context of other Acts using the phrase carrying on business, some guidance can be found in a Fact Sheet issued by the Attorney-General's Department in the context of the Privacy Amendment (Private Sector) Bill 2000. There it is noted that:

> In order to regulate the behaviour of foreign organisations operating outside Australia *it is necessary to establish a strong link with Australian jurisdiction*. In the Bill that link is based on a range of factors. The foreign organisation must carry on business in Australia and deal with information about Australians. The information must have been collected, or held at some time, in Australia. For example, where a foreign company collects information about Australians in Australia and then moves that information overseas, the company will have to apply the safeguards set out in the Bill.[27] (emphasis added)

The reference to the need for a 'strong link with Australian jurisdiction' could be read to exclude the possibility of the Act being applied extraterritorially in single contacts between the offender and the data subject. However such an interpretation may not be wise from a policy perspective (see below).

Collected or held by the organisation in Australia

Turning to the question of whether personal information was 'collected or held' by the organisation *in Australia*, we need to discuss collection and holding separately. Of the two terms, the definition of 'held' ought to be least controversial. Information would presumably be regarded as being held at the location it is physically stored. For example, where a foreign corporation stores the information on a server in Australia, that information is likely to be 'held' in Australia. Alternatively, focus may be placed on some aspect of the location of the organisation in question. For example, one approach would be to say that regardless of where the information is physically stored it is regarded as being 'held' at the place where the organisation has its main place of business. Both of these alternatives are workable, and both are associated with weaknesses. While having the advantage of being the actual location the

[27] 'Fact sheets from the Attorney General's Department', 2000 *Privacy Law and Policy Reporter* 13. <http://beta.austlii.edu.au/au/journals/PLPR/2000/13.html> (last visited 15 February 2007).

information is 'held', focusing on the location of a server is always going to be difficult; content is easily moved from one server to another, servers may be moveable, and organisations may be tempted to choose to store information on servers in so-called data-havens (i.e. places with little or no regulation of data processing). Focusing on the location of the organisation's main place of business has the advantage of being less susceptible to manipulation by the organisation, but on the other hand, such a focus is just a legal fiction, and it can legitimately be questioned whether the legislator had such an interpretation in mind when drafting s. 5B.

When it comes to the question of under which circumstances it could be said that personal information was 'collected' by the organisation *in Australia* in the context of the Internet, we are faced with the classic dilemma of where Internet communications 'take place'. That is; does eg a website visitor 'go' to the server hosting the website, or does the operator of the website 'go' to the website visitor. The first thing to note for the purpose of identifying where 'collection' takes place is that, while the general issue of where Internet communications take place has been discussed extensively in the context of contracts concluded via the Internet, no guidance can be drawn from this discussion owing to the contract law specific rule that a contract is concluded at the place of the last act necessary for the conclusion of the contract. Further, while the issue of where Internet communications take place is a conceptual question without an obvious answer, it is a question of great importance – if we conclude that the website visitor goes to the website, it would follow that personal information was not collected by the organisation *in Australia*. However, if we conclude that the website operator goes to the website visitor, it would follow that personal information was, indeed, collected by the organisation *in Australia*. As both of these alternatives are equally arguable from a technical perspective, the question must necessarily be determined by reference to which of the alternatives we think provide the better outcome.

The policy considerations

In light of the above, both the definition of 'carrying on business', and the definitions of when information is 'collected or held' *in Australia* must depend on what objectives we wish to achieve. In this context, that means that when charged with the task of determining the definition of 'carrying on business' and the definitions of when information is 'collected or held' *in Australia* one must, by reference to policy considerations, evaluate whether it is preferable to make the *Privacy Act*'s extraterritorial reach wide or narrow. Should it be preferable to give the *Privacy Act* a wide extraterritorial scope, we may conclude that an organisation is *carrying on business in Australia* whenever it interacts (whether directly commercially or not) with

an Australian citizen or another person whose continued presence in Australia is not subject to a limitation as to time imposed by law. Further, we may also conclude that information is collected *in Australia* where the data subject is located in Australia at the time of collection, and that information is held *in Australia* where it is either physically stored in Australia, or the organisation holding the information is based, wholly or in part, in Australia. However, should it be preferable to give the *Privacy Act* a narrow extraterritorial scope, we may conclude that an organisation only is *carrying on business in Australia* if it has a continuous and systematic commercial presence in Australia. Further, to give the *Privacy Act* a narrow extraterritorial scope, we may decide that information is collected *in Australia* only where the data collector is located in Australia at the time of collection, and that information is held *in Australia* only where it is physically stored in Australia.

So what are the relevant policy considerations? Starting with the consequences of choosing a narrow approach, the most obvious disadvantage is that Australians may be relatively unprotected against privacy violation made by overseas organisations. This is a very serious concern on an increasingly global market. Imagine, for example, an Australian resident coming across a particular website while surfing the net. The website offers free medical advice where the visitor provides a list of her/his symptoms. Imagine further that the operators of the website, without the website visitors' knowledge or consent, sells the sensitive health information gathered to a drug company, or perhaps even worse publishes the information on its website.

Should it be the case that the website eg contained a misleading privacy statement, it may be possible for the Australian person in question to take action under s. 52 of the *Trade Practises Act 1974* (Cth), arguing that the foreign business has engaged in misleading and deceptive conduct. However, it could be seen as inappropriate that no protection would be afforded under the Australian privacy regulation. The example also illustrates how single interactions can have serious privacy implications, which indicates that it would be misguided to require the repetition of acts for an organisation to be 'carrying on business' in Australia. Similarly, in light of the serious effects that may flow from single interactions, it may not be advisable to read the 'carrying on business' test as requiring the activity to possess a permanent character. Furthermore, taking a narrow approach to the extraterritorial scope of the *Privacy Act* would doubtlessly encourage the use of data havens as discussed above.

Apart from the avoidance of the negative consequences of taking a wide approach, there are no real positive consequences of taking a narrow approach. While that may seem to indicate that the wider approach is superior, such a conclusion should not be reached without first examining the negative consequences of taking a wide approach.

First, it could be argued that Australian law should only regulate acts done, or conduct occurring, in Australia. Giving a wide scope to the definition of 'carrying on business', and the definitions of when information is 'collected or held' *in Australia* would arguably not be in line with such a goal. At the same time, however, it should be noted that, as mentioned above, a wide approach does not appear to be contrary to public international law, and as foreign states have the choice to refuse to cooperate (eg with enforcement) the international system is, in a sense, self-correcting. Further, Australia like many other countries is already making wide extraterritorial claims. For example, in *Dow Jones & Company Inc v Gutnick*[28] the High Court ruled that in publishing an article on a website hosted in the US, the publisher Dow Jones & Company Inc came under Australian jurisdiction and Australian law, since the relevant website was accessed from Australia. In other words, focus was placed on the location of the people downloading and reading the article rather than on the location of the people uploading it.

It must be remembered that the outcome in the *Gutnick* case can be attributed to the peculiarities of defamation law. However, if wide jurisdictional claims can be made in the context of eg defamation, there are no obvious policy reasons why such claims cannot also be made in the context of privacy.

A second concern with giving the *Privacy Act* a wide extraterritorial applicability is that where such applicability cannot be backed up by effective enforcement, the making of the extraterritorial claims may have a negative effect. As noted by one learned commentator the main problem is not necessarily the regulatory overreaching itself, but the risk that ineffective enforcement makes a mockery of the law.[29] While there certainly is force in this argument, it must be remembered that regulatory leakage is commonplace. For example, despite more and more speed cameras, only a small portion of those driving faster than allowed on our roads are caught, but the speeding laws are nevertheless useful or even necessary. Indeed, if regulatory leakage is commonplace in domestic law, it is even more so in the cross-border context. There are countless examples of judgments rendered in one state not being enforced in another,[30] and had the US courts been asked to enforce an Australian court's judgment awarding damages to Mr Gutnick in the Internet

---

28 (2002) 210 CLR 575.

29 L. Bygrave, 'Strengthening privacy protection in the Internet environment: A modest program of action' 2006 *Privacy Law and Policy Reporter* 2006 11, at. 222-226.

30 See eg *Yahoo!, Inc. v La Ligue Contre Le Racisme et L'Antisemitisme*, 169 F.Supp. 2d 1181 (N.D. Cal. 2001).

defamation dispute mentioned above, they would have been likely to refuse to do so.[31]

While it seems possible to counter the two first arguments against giving the *Privacy Act* a wide extraterritorial reach, the third is more difficult to address – giving the *Privacy Act* a wide extraterritorial reach encourages the use of geo-identification techniques. Geo-identification is the practise of eg website operators identifying the geographical location of those visiting their websites.[32] Typically, the identification is based on the IP addresses assigned to the visitor's computer, and works as follows: As your web browser sends a request to access a particular website, it includes amongst other things, your IP address. The server hosting the relevant website passes on your IP number to a provider of a geo-location service, in what can be called a 'location request'. Having built up a database in which IP addresses are matched to geographical locations, the provider of the geo-location service is able to make an educated guess as to your location. This information is passed on to the server hosting the relevant website in what can be called a 'location reply', and armed with this information the server hosting the relevant website can determine whether or not it will allow you to access the website, or eg what type of advertisement will be displayed on the website.

Should the *Privacy Act* be given a wide scope of application, it will inevitably encourage the use of geo-identification techniques – after all, with a widely applicable *Privacy Act*, a website operator can only assess whether it will be exposed to Australian privacy regulation by knowing the geographical location of the data subject. As the use of geo-identification techniques becomes more widely used, the Internet will be transformed from the virtually borderless medium we know today, to something that more resembles our physical world divided by borders of different kinds.[33] In this context it needs to be noted that:

- A wide adoption of geo-identification techniques may be unavoidable anyhow in light of their usefulness for eg targeted advertisement and fraud prevention; and

---

31 For an in-depth discussion on the gap between jurisdictional claims and courts' willingness to recognise and enforce foreign judgments, see: D. Svantesson, *Private International Law and the Internet*, (Alphen aan den Rijn: Klüwer Law International, 2007), at 50-53.

32 See further: Dan Svantesson, 'Geo-location technologies and other means of placing borders on the "borderless" Internet' *John Marshall Journal of Computer & Information Law*, Vol XXIII, No 1, Fall 2004.

33 One interesting example is the website of US TV organisation Showtime Online. If one visits <www.sho.com> while outside the US, one is greeted by the following: 'Sorry. We at Showtime Online express our apologies; however, these pages are intended for access only from within the United States.' (last visited 21 February 2007).

- Many other areas of law, such as the regulation of defamation and online gambling, already work to make necessary the use of geo-identification techniques.

However, it must be questioned whether the fact that also other factors contribute to the widespread use of geo-identification, can be said to justify the *Privacy Act* being structured in a manner that encourages the destruction of one of the Internet's greatest features – its 'borderlessness'.

Consequently, whether we ought to give the *Privacy Act* a wide or narrow extraterritorial scope is a pure policy question. Both alternatives are possible, and associated with advantages and disadvantages.

The practical function of s5B

One final issue most be addressed. If it is suggested that provisions like s5(1) of the TPA and s5B of the *Privacy Act* do not determine the question of jurisdiction, as was held in *Bray v F. Hoffman-La Roche Ltd*, we must ask how the issue of jurisdiction is determined, and what, if anything, in the conflict of laws context do such articles determine. The first of these sub-questions is relatively easy to answer; a court seeking to exercise jurisdiction over a party that has acted in violation of the *Privacy Act* would need to ensure that the action fits under one of the jurisdictional grounds available to that court.[34] While such a scenario may arise where a party is seeking an injunction eg restraining a privacy violation, the more normal scenario would be that a complaint is made to the Privacy Commissioner, and in this latter case, it would be the provisions of the Privacy Act regulating the role of the Privacy Commissioner that would be of relevance. The answer to the second sub-question will depend on whether an action is taken in a court (i.e. an injunctions action) or a complaint is made to the Privacy Commissioner. Where the dispute comes before a court, the rule expressed in s5B could, in a sense, be seen as a *de facto* choice of law rule – having determined that it can exercise jurisdiction under the relevant jurisdictional rules, the court would use s5B to determine whether the *Privacy Act* is applicable to the foreign party's conduct. In contrast, where the dispute comes before the Privacy Commissioner there is no choice of law issue as the Privacy Commissioner can only act under the *Privacy Act*. However, while not a choice of law, where the dispute comes before the Privacy Commissioner, s5B works as a measure for determining the question of jurisdiction; that is, whether or not the claim falls within the Privacy Commissioner's jurisdiction.

---

[34] D. Svantesson, *Private International Law and the Internet*, (Alphen aan den Rijn: Klüwer Law International, 2007), at 92-107.

Transborder data flow

Without adequate protection against transborder data flow, privacy regulation would arguably be pointless as personal information simply would be transferred to other jurisdictions without privacy protection. Of course, rules against the disclosure of personal information could prevent some such transfer, but it is nevertheless submitted that the approach of specifically regulating transborder data flow, taken eg in the Australian *Privacy Act*, is a correct one in today's global world. At the same time, while National Privacy Principle 9 (which regulates transborder data flow) contains many appropriate features, it does not adequately protect data subjects where personal information is transferred to another jurisdiction. Furthermore, NPP 9 could usefully be modified to better support the fulfilment of certain desirable policy objectives.

NPP 9 reads as follows:

> An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:
>
> (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; or
>
> (b) the individual consents to the transfer; or
>
> (c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or
>
> (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or
>
> (e) all of the following apply:
>
> (i) the transfer is for the benefit of the individual;
>
> (ii) it is impracticable to obtain the consent of the individual to that transfer;
>
> (iii) if it were practicable to obtain such consent, the individual would be likely to give it; or
>
> (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.

The role of the Privacy Commissioner

The first problem I note with NPP 9 does not stem from the provision itself, but rather from the approach taken by the Privacy Commissioner. Unlike the approach taken in Europe, the Privacy Commissioner does not identify states with privacy protection meeting the test of a "substantially similar" privacy protection outlined in NPP 9(a). This is undoubtedly a concern as it means that (1) each individual organisation has to make a costly assessment as to whether the privacy regulation of other jurisdictions meet the test of the *Privacy Act*, and (2) leaving the assessment to the organisations that benefit from the transfer encourages a very generous definition of what can be regarded as substantially similar privacy protection – it simply is not in the interest of an organisation wishing to transfer personal information to be restrictive in its assessment of whether the privacy regulation of a country to which transfer is desired is substantially similar to that of Australia.

The better approach would be for the Privacy Commissioner to identify countries that meet the requirement of having a substantially similar privacy regulation. In doing so, the Privacy Commissioner would provide for greater clarity and certainty. Further, this approach would greatly benefit organisations engaged in transborder data flow as it would be easier for them to know which other states can be said to have a substantially similar privacy regulation to that of Australia. Indeed, the cost to society of each organisation engaged in transborder data flow having to ascertain whether the country in question meets the test set out in NPP 9(a) is extraordinarily high, compared to the cost to society of the Privacy Commissioner identifying those countries. Finally, individuals would benefit from the impartial assessment of the Privacy Commissioner as compared to the assessment made by organisations wishing to transfer personal information.

At the time when the Privacy Commissioner has made its assessment of which countries' privacy regulation is substantially similar to that of the NPPs, the undesirably weak focus in NPP 9(a) placed on the organisations' reasonable beliefs will no longer be necessary.

Furthermore, the Privacy Commissioner outlining a list of countries meeting the test set out in NPP 9(a) has several policy benefits. The main benefit is that by listing countries with adequate privacy protection, one arguably makes it easier for Australian organisations to cooperate with organisations from those countries, over organisations from other countries. This can potentially have the effect of encouraging data processing countries currently lacking adequate privacy regulation, like India, to implement appropriate privacy protection. In other words, NPP 9 could usefully be changed to support the fulfilment of important policy objectives. At the same time, it must be recognised that transborder data flow regulation may

contribute to the digital divide. Thus, states like Australia should offer assistance for developing countries to develop appropriate privacy regulation.

Consent – the miracle cure for violations

Having said this, the undoubtedly greatest weakness of the approach taken in NPP 9 stems from the *Privacy Act*'s approach to consent. To put it bluntly, consent is the miracle cure that cures virtually any abuse possible under the NPPs. The motivation for this is presumably found in the law seeking to provide for party autonomy – if an individual wishes an organisation to treat her/his personal information in a particular manner, and the organisation wishes to treat that individual's personal information in that particular manner, then the law should not stand in the way. This approach has a logical appeal, but is fundamentally flawed in any system were the requirement for a valid consent is not strong enough; and the Australian *Privacy Act*'s approach to consent is weak indeed. This is so partly because the definition found in the Guidelines accompanying the Private Sector Amendment to the *Privacy Act* (the September Guidelines) watered down the requirement originally proposed in an earlier version of the Guidelines (the May Guidelines).[35] For example, while the May Guidelines took a rather strict approach to so-called implied consent, the September Guidelines are much more lenient. The May Guidelines stated that '[g]enuine consent can only be implied in circumstances where it is clear that a person knows and understands what they are consenting to and clearly indicates from their behaviour that they have agreed'.[36] In contrast the September Guidelines simply states that '[i]mplied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the organisation'.[37]

For it to be justified that consent is treated like the 'miracle cure' it currently is, consent should only be valid were it is:

1. identifiable;
2. informed;
3. variable; and
4. given freely.

---

[35] See further: D. Svantesson, ' "Consent" - How much can the meaning of a word change in four months?', 2001 *Privacy Law & Policy Reporter*, 8, at 112 – 113.

[36] 'Draft Guidelines to the National Privacy Principles' (May 2001). <http://www.privacy.gov.au/publications/dnppg.html> (last visited 25 February 2007).

[37] 'Guidelines to the National Privacy Principles' (September 2001), at 22. <http://www.privacy.gov.au/publications/nppgl_01.pdf> (last visited 25 February 2007).

The first requirement, that consent be identifiable, simply means that whether expressed or implied, the organisation arguing that consent was given must be able to point to an act that indicates the consent being given. This requirement is typically not a problem, and can easily be met eg by requiring a signature, or by taking a bit of care when relying on implied consent.

It is submitted that consent, in the context of transborder data flow, is rarely sufficiently informed. For example, it cannot be said that informed consent was given where an individual agrees to her/his personal information being transferred overseas without knowing to which country the transfer is to take place. An organisation seeking consent to transfer personal information to another country should be required to inform the data subject of which country the transfer relates to and how the personal information will be protected there.

The third requirement simply means that consent that has been given must be revocable – the data subject must be allowed to change her/his mind. Obviously, where that happens, the organisation must be given a reasonable amount of time to respond to the revocation.

The final requirement of consent being given freely is rarely disputed. However, in practice it is not always easy to say that consent has been given freely. For example, organisations often engage in the practice of bundling consent; that is, in consenting to one form of data processing, the data subject must also consent to a wide variety of other forms of data processing. While the practice of bundling has its uses, it is clearly being misused, and as a consequence data subjects are faced by take it or leave it options where a more appropriate approach would have allowed them to interact with the organisation without consenting to a range of secondary uses of their personal information. In bundling consent, the primary use should always be clearly separated, and any secondary uses sought should be bundled in categories, if bundled at all.

The weakness of the consent requirement is arguably illustrated in the only reported decision of the Privacy Commissioner that deals with the relevant aspect of NPP 9. In *E v Money Transfer Services* [2006] PrivCmrA 5 the Privacy Commissioner held that the complainant had impliedly consented to the overseas transfer of personal information. However, as is reflected in the very fact that a complaint was made, that implied consent may not have been particularly informed.

Strict liability for data exporters

Even with a tightening up of the consent rules, at least one more change could usefully be made to improve the effectiveness of NPP 9. Both the Asia-Pacific Economic Cooperation Privacy Framework[38] and the Asia-Pacific Privacy Charter[39] include provisions to the effect that the exporter of personal information is accountable for how the information is treated once it leaves the exporter's territory. This is an excellent idea that should be incorporated into NPP 9. Indeed, it is submitted that NPP 9 usefully could include a strict liability for the data exporter.

Placing a strict liability on the data exporter ensures that the data subject has easy access to redress – there would be no need to seek protection under the, possibly weak, foreign privacy law. At the same time, the data subjects are to have the right to seek redress from the party who is directly responsible for the breach, should they wish to do so. Further, businesses exporting data must inform the data subjects of their rights. While this approach may seem rather onerous, organisations can mitigate the effect of the above mentioned liability through contractual arrangements with the receiver of the personal information. Further, by imposing this liability, it can be anticipated that data exporters will take greater care in selecting to whom they will export personal information.

The e-mail problem

While, as outlined above, it seems clear that it is necessary to regulate transborder data flow, it is equally clear that such regulation is not easily applicable in relation to communication occurring on a global computer network. One problem arises in the context of e-mails containing personal information, being sent by, or to, e-mail systems hosted overseas. This problem is augmented by the fact that, the laws of the place where the e-mail system server is located may require that the authorities have access to the e-mails and thereby the personal information. Imagine, for example, a situation where an Australian doctor emails some test results to an Australian patient. Imagine further that the patient is using Microsoft's Hotmail system. While the e-mail is sent from one Australian party to another, the e-mail including the sensitive personal information it contains, may be stored on a server overseas. Has the Australian doctor in this situation transferred personal information to someone in a foreign country? The answer would seem to be yes, as the information is placed on a server located in a foreign country. The next question is then whether the doctor has acted in violation of NPP 9 in doing so? In answering this latter question, one

---

38 Asia-Pacific Economic Cooperation, '*APEC Privacy Framework*' (2005), [48].

39 Asia-Pacific Privacy Charter Council, '*Asia-Pacific Privacy Charter*', Privacy Principle 12.

could point to the fact that the patient voluntarily has chosen the e-mail system it uses which could be seen as an indication of consent to the transfer. However, first of all, it may be likely that the patient was unable to properly appreciate the consequences of doing so, and thus we can question whether such consent was informed. To make such consent informed, the organisation should take steps to ensure that the patient fully appreciates the consequences of using e-mail for the communication. Indeed, in many situations, e-mail simply is not a suitable form of communication due to its inherent openness. Further, should the scenario be slightly different so that it involved one doctor e-mailing the test results to another Australian doctor (an act that would be regulated by NPP 2's rules on disclosure), the patient may have consented to the disclosure, but not to the transfer to another country.

The problem outlined above does not have a simple solution. One possibility would be to make an assessment of the reasonableness of the organisation's actions in arguably exporting the personal information. Both the advantages and disadvantages of such an approach would flow from its flexibility. While the approach would be flexible enough to protect organisations acting reasonably in a wide range of circumstances, it would also be uncertain enough to make it virtually impossible for a data exporter to know whether it has acted in violation of NPP 9. The only way to make this approach work would be by providing extensive guidelines.

Another possibility is simply to view such an act as involving transfer to a third country. It would then be for the organisations regulated by the Act to make sure that they avoid such situations by using an e-mail system that does not involve the e-mails being stored on a server located in a foreign country. While this may incur some costs for the organisations, it must be remembered that as currently drafted, the *Privacy Act* only applies to large organisations (with an annual turnover of more than $3 million), and such organisations that deal with sensitive personal information such as health information.

It has sensibly been suggested that the scope of the Act should be expanded so as to abandon the $3 million test.[40] Should that be done, the issue outlined above may become more difficult to address with the latter of the two possible solutions canvassed above no longer being a viable alternative. However, it is submitted that, should the *Privacy Act* be expanded to cover also small businesses and individuals, the NPPs may have to give way to an abuse regulation, similar to that in place in

[40] See eg the Australian Privacy Foundation's submission at 13-14 <http://www.privacy.org.au/Papers/ALRC_IP31_070202.pdf> (last visited 25 February 2007).

Swedish privacy law,[41] at least in relation to individuals but possible also smaller organisations.

A detailed discussion of this abuse regulation goes beyond the scope of this article, but put simply, the Swedish privacy law exempts from its normal regulation, processing of personal information where the personal information is not included in, and not intended to form part of, a structured collection of personal information.[42] Such data processing is only subject to abuse rules. In other words, that type of processing is allowed provided that it does not amount to an abuse of the personal integrity of the data subject(s). It is acknowledged that there can be no clear rules as to when such a violation has taken place, but most people would instinctively know the boundaries, and any assessment would have to take account of all the circumstances including: the purpose for the processing, the context of the processing, the spread of the processing and the likely consequences of the processing. In providing guidance for assessing whether or not data processing amounts to abuse, *Datainspektionen*[43] states that, for example, the data must not be processed (1) for the purpose of harassment, stalking or scandalising the data subject, (2) in great quantities about a data subject without there being a legitimate reason for the processing, (3) in a defamatory manner or (4) in a manner that violates confidentiality.[44] Finally, the data subject must have the right to have inaccurate information corrected.[45]

It is clear that Australian law, eg defamation law and confidentiality law, already protects aspects of what is classed as abusive processing of personal information. However, it is submitted that there nevertheless would be advantages in adopting a model similar to that in place in Sweden. One such advantage is found in the comparative accessibility of the complaints process in place in relation to the *Privacy Act* – while most people would be very hesitant to instigate a costly defamation proceeding, making a complaint to the Office of the Privacy Commissioner is a much more realistic avenue to redress.

---

41 Personuppgiftslag (1998:204) as amended.

42 Personuppgiftslag (1998:204), 5 a §.

43 The Swedish data protection authority.

44 See further: Datainspektionen's "Questions and Answers", Question 5 <http://www.datainspektionen.se/fragor_svar/personuppgifter/ny_pul5.shtml> (last visited 25 February 2007).

45 See further: See further: Datainspektionen's "Questions and Answers", Question 5 <http://www.datainspektionen.se/fragor_svar/personuppgifter/ny_pul5.shtml> (last visited 25 February 2007).

Concluding remarks

This article has given attention to some crucially important aspects of the regulation of privacy – the international aspects. The two main international aspects of privacy regulation – extraterritorial application, and transborder data flow – were discussed and analysed. While this was done in the context of the Australian *Privacy Act 1988* (Cth), much of the discussion above ought to be relevant also in relation to the privacy regulation of other states.

The regulation of privacy is changing and developing in many countries, and indeed, the Australian privacy regulation is in a state of flux – not least due to the Australian Law Reform Commission's commendable initiative of having an inquiry focused on the *Privacy Act*. In light of that, some suggestions were made as to how these issues could be regulated. However, the most important function of this article is to highlight the issues and bring attention to the policy considerations involved. I will follow the development of cross-border privacy regulation with great excitement.