PRIVACY, THE INTERNET AND TRANSBORDER DATA FLOWS

AN AUSTRALIAN PERSPECTIVE*

by

DAN JERKER B. SVANTESSON**

Cross-border transfer of personal information is now more common than ever before. Indeed, modern technologies like the Internet would simply not work in the absence of such transfers. At the same time, cross-border transfer of personal information is associated with serious privacy risks.

Taking an Australian perspective, this paper examines how the law seeks to balance these two considerations – the need for transfer, and the need for privacy protection.

KEYWORDS

Privacy, data protection, Internet, transborder data flows, Australia

1. INTRODUCTION

No one would have failed to observe the Internet's enormous ability to facilitate communication across geographical borders – in the absence of specific technology, the 'net' does not even recognise the existence of geographical borders. In sharp contrast, the protection of privacy – a widely recognised fundamental human right[1] – is so far wholly dependent on information being kept within geographical borders.

---

* This article draws, and expands, upon a range of the author's previous work on the regulation of transborder data flows. In particular Svantesson, D. 2007, 'Protecting privacy on the "borderless" Internet – Some thoughts on extraterritoriality and transborder data flow', *Bond Law Review,* vol. 19, no. 1, pp. 168 – 187, and the author's submission of December 2008 to the Department of the *Prime* Minister and Cabinet on the proposed UPP 11 have been relied upon.

** Associate Professor, Faculty of Law Bond University, Gold Coast Queensland 4229 Australia, Ph: +61 7 5595 1418, E-mail: Dan_Svantesson@bond.edu.au, (http://www.svantesson.org).

1 See primarily the International Covenant on Civil and Political Rights and the European Convention on Human Rights.

Despite this apparent opposition, there is remarkably little literature and cases dealing with privacy protection in the context of transborder data flows on the Internet. This paper examines how Australia is proposing to regulate privacy in relation to transborder data flows on the Internet. It also discusses the challenges any such regulation necessarily must be able to address. However, first, it is necessary to set the scene by saying a few words about why such regulation is needed.

2. WHY IS THERE A NEED FOR REGULATION?

Seeing how some countries completely lack privacy regulation, the regulation of the circumstances under which personal information or data may be transferred to another country may, at a first glance, seem like a small concern. However, the truth is that it is that very fact – the complete lack of privacy regulation in many countries around the world – that makes the regulation of transborder data flow crucially important. The truth of the matter is that, due to the present primitive and underdeveloped structure for cross-border protection and enforcement of privacy rights, the transfer of personal data to another country represents an abandonment of the protection afforded under local law. In other words, where personal information about a person in one country is transferred outside that country, the person in question often looses any realistic opportunity to control how that information is used. The fact that many privacy regulations claim to have extraterritorial effect is of little practical significance due to lacking enforcement.

These serious consequences must be balanced with the Internet's inherent need for transborder data flows.

3. THE AUSTRALIAN APPROACH

Australia is currently in the middle of a major overhaul of its entire privacy regulation. After extensive consultation, the Australian Law Reform Commission presented its findings regarding privacy regulation in May 2008. The 2,694 page document outlined 295 recommendations. The Australian Government is currently working its way through those recommendations. At the time of writing, the Government has just released its response to 197 of the recommendations, accepting 141 of them either in full or in principle and accepting another 34 with qualifications. The responses to the remaining 98 recommendations – many of which are crucial for the overall operation of the regulatory system – will be presented during the second stage of the process.

One of the recommendations that has been considered, and that has been adopted with amendments, is Recommendation 31-2 which relate to trans-

border data flow. That recommendation is discussed in detail below, but to put that recommendation in its proper context, it is first necessary to examine how Australia so far has regulated transborder data flow.

4. TRANSBORDER DATA FLOW UNDER THE CURRENT PRIVACY REGULATION

On 21 December, 2001, Australia's *Privacy Act 1988* (Cth) was amended so as to also regulate the private sector. The most important aspect of the private sector regulation was the incorporation of ten National Privacy Principles (NPPs) that private sector organisations captured by the legislation need to follow. NPP 9 addresses transborder data flow:

> *NPP 9*
>
> *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.*

As I have pointed out elsewhere, this provision is far from perfect and suffers from a range of defects.[2]

4.1. CONSENT

Under NPP 9, as is the case in relation to several of the NPPs, 'consent' is a miracle cure for virtually any abuse imaginable.[3] As people in general are unable to assess the risks associated with a transfer of their personal information to another country, consent given is typically not sufficiently informed - it would be naive to think that the average consumer ever could fully evaluate the legal implications of consenting to their personal information being transferred overseas. However, there can be no doubt that much more could be done to ensure that data subjects are informed about the risks involved.[4]

Furthermore, data exporters often make matters worse bundling consent for transfer to a third country with consent for other uses. Such bundled consent may be justifiable in some context, but never in relation to overseas transfer of personal information. Based on the above, a provision regulating transborder data flows should make clear that consent is ineffective if bundled with consent for other issues. Finally, as far as consent is concerned, for consent to be valid, the data subject must, for example, be informed of:

> *(a) the country or countries which are the destination(s) of the transfer;*
>
> *(b) the intended recipient(s);*
>
> *(c) the protective measures that will be taken in relation to the personal information;*
>
> *(d) how the personal information will be used at the destination; and*
>
> *(e) whether the personal information will be transferred from the destination country (where the personal information will be transferred from the destination to a third country, all the information outlined here must also be provided in relation to the third country).*

---

[2] Svantesson, D. 2007, 'Protecting privacy on the "borderless" Internet – Some thoughts on extraterritoriality and transborder data flow', *Bond Law Review,* vol. 19, no. 1, pp. 168 – 187.

[3] 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 sufficiently informed.

[4] Perhaps the very confronting warnings placed on cigarette packs in Australia (see further: http://www.smoke-free.ca/warnings/australia-warnings.htm [Accessed 29 November 2009]) could serve as an example of how consumers can be informed of the risks involved in allowing their personal information be transferred to another country?

4.2. REASONABLE BELIEF

There is absolutely no justification for placing emphasis on whether the organisation responsible for the transfer "reasonably believes" that adequate protection would be afforded after the transfer. The reference to a "reasonable belief" creates a significant, and unnecessary, uncertainty without adding any benefits. The appropriate approach would be to require the organisation in question to meet a higher standard of proof by asking them to show that show that the recipient of the information is subject to a law or binding scheme which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles. While, at a first glance, the difference between requiring a 'reasonable belief' and requiring proof that an adequate level of protection will be provided may seem minimal, an example may illustrate the enormous practical differences.

Imagine that company A wishes export data to country X. It contacts a privacy consultant (or a law firm) asking the consultant to assess whether a recipient in country X is subject to a law or binding scheme which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles. The consultant writes a statement to the effect that such a law or binding scheme is in place in country X. Imagine further that it turns out that the advice is incorrect, that country X lacks adequate privacy protection and that a data subject suffers loss due to the fact that company A exported their personal information to country X.

If in this scenario the regulation of transborder data flows merely requires a reasonable belief, company A has surely met the test. Indeed, the ALRC Report makes clear that legal advice is sufficient.[5] As a consequence, the affected data subject can make no claim against company A. This has the flow on consequence that, since company A has not suffered any harm from the consultant's poor advice it may not have much of a case to make against the consultant.

In contrast, if the regulation of transborder data flows requires company A to show that the recipient in country X is in fact subject to a law or binding scheme which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles, company A would be unable to do so in our scenario. As a consequence, the data subject can take action against company A, and company A can, in

[5] Australian Law Reform Commission 2008, *For Your Information: Australian Privacy Law and* Practice, Report No 108, Australian Government, Canberra, para. 1100.

turn, make a claim against the consultant for e.g. negligent misrepresentation or a breach of section 52 of the *Trade Practices Act 1974* (Cth).

As can be seen from this example, the practical consequences are dramatically different, and if one allows oneself to be cynical, it is not difficult to see why some law firms and privacy consultants, as well as data exporting organisations, would be very eager to avoid a change from the inadequate 'reasonable belief' test.

4.3. SUBSTANTIALLY SIMILAR

Considering that Australia's approach does not represent international best practice, it could be said to be somewhat arrogant to focus on a "substantially similar" privacy protection instead of acknowledging that there may in fact be a better privacy protection scheme in the country to which the data is transferred. Consequently, the regulation of transborder data flows must be structured to ensure that a transfer allowed under a scheme that provides for "substantially similar" protection, also is allowed under a scheme that provides a more favourable protection for the data subject.

Unlike the approach taken in Europe, the Australian Privacy Commissioner does not identify states with privacy protection meeting the test of a "substantially similar" privacy protection outlined in NPP 9(a). The benefits of a 'white list' are well documented, and the Australian Government should develop and publish a list of laws and binding schemes in force outside Australia that effectively uphold principles for the fair handling of personal information that are substantially similar to, or better than, those in place in Australia.

4.4. ACCOUNTABILITY

Furthermore, unlike both the Asia-Pacific Economic Cooperation Privacy Framework[6] and the Asia-Pacific Privacy Charter[7] NPP 9 does not 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. While, as is discussed above, there are limits to the usefulness of accountability provisions, such a provision would have strengthened NPP 9. However, this accountability must necessarily be combined with the type of 'border protection' catered for under the NPP 9.

---

[6] Asia-Pacific Economic Cooperation 2005, *APEC Privacy Framework,* APEC Secretariat, Singapore, para. 48.

[7] Asia-Pacific Privacy Charter Council 2003, *Asia-Pacific Privacy Charter*, Privacy Principle 12.

4.5. IN A FOREIGN COUNTRY

Finally, the wisdom of referring to transfer to someone "in a foreign country" may be questioned. The reference to a foreign country seems to suggest that transfer to a location outside Australia, that is not a country, is beyond the regulation of NPP 9. This opens the door for transferring personal information to data processing facilities located in an international space such as the high seas, which obviously can be just as harmful as transfer to a foreign country. While the idea of data havens in intentional spaces may seem far-fetched, attempts have, in fact, already been made at establishing hosting facilities beyond the reach of any country's jurisdiction.[8] Further, Google is pursuing the idea of offshore data storage centres.[9] Consequently, the risk is not as remote as might first be though.

5. TRANSBORDER DATA FLOW UNDER THE PROPOSED PRIVACY REGULATION

While the Government is yet to express this recommendation in the form of legislation text, it has made clear its intention to follow all the major aspects of the ALRC's recommendation regarding transborder data flows. Combining the ALRC's proposal with the comments made in the Government's response, Unified Privacy Principle 11 (UPP 11) is likely to look something like this:

> *UPP 11*
>
> *11.1 If an agency or organisation in Australia or an external territory transfers personal information about an individual to a recipient (other than the agency, organisation or the individual) who is outside Australia and an external territory, the agency or organisation remains accountable for that personal information, unless the:*
>
> *(a) agency or organisation reasonably believes that the recipient of the information is subject to a law or binding scheme which effectively upholds privacy protections that are substantially similar to these principles;*
>
> *(b) individual consents to the transfer, after being expressly advised that the consequence of providing consent is that the agency or organisation will no*

[8] Refer e.g. to the now failed data haven, HavenCo, located on an abandoned anti-aircraft platform. Garfinkel, S. 2000, 'Welcome to Sealand. Now Bugger Off', Wired, issue 8.07, http://www.wired.com/wired/archive/8.07/haven.html [Accessed 27 November 2009].

[9] Miller, R. 2008, 'Google Planning Offshore Data Barges', *Data Centre Knowledge*, http://www.datacenterknowledge.com/archives/2008/09/06/google-planning-offshore-data-barges/ [Accessed 29 November 2009]. See further: Clidaras, J., Stiver, D. W. & Hamburgen, W. 2008, *Water Based Data Center*, US Patent Application 20080209234, http://appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220080209234%22.PGNR.&OS=DN/20080209234&RS=DN/20080209234 [Accessed 29 November 2009].

> *longer be accountable for the individual's personal information once transferred; or*
>
> *(c) agency or organisation is required or authorised by or under law to transfer the personal information;*
>
> *(d) the agency or organisation reasonably believes that the disclosure is necessary to lessen or prevent a serious threat to:*
>
> *(i) an individual's life, health or safety; or*
>
> *(ii) public health or public safety;*
>
> *where in the circumstances, it is unreasonable or impracticable to seek the individual's consent;*
>
> *(e) the agency or organisation has reason to suspect that unlawful activity or serious misconduct has been, is being or may be engaged in, and the disclosure of the personal information is a necessary part of its own investigation of the matter or in reporting its concerns to relevant persons or authorities; or*
>
> *(f) the agency or organisation reasonably believes that the disclosure is necessary for the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law.*

First of all it is interesting to observe that UPP is very different to all the other UPPs – it is "unbreakable". While data processor may act in a manner that violates any of the other UPPs, it is simply impossible for a data processor to violate UPP 11. If transfer tales place outside the wide scope of the types of transfer anticipated in sub-sections a-f, the data processor will be accountable for the actions of the receiver. This fundamental difference between UPP 11 and the other UPPs has not been explored, nor has it been explained, by either the ALRC or the Australian Government.

The change from NPP 9 to UPP 11 carries with it a terminology change. Instead of referring to the area as transborder data flows, it is now referred to as cross-border data flows. More importantly, the new approach to regulating this area, whatever you call it, will involve the Office of the Privacy Commissioner publishing a list of laws and binding schemes that meet the test of being providing privacy protection substantially similar to the UPPs.[10] Further, the new wording avoids the risk of exports to data havens in international spaces being exempt. Another positive step is taken in that

[10] Australian Government 2009, *First Stage* Government Response to the ALRC Report 108, Australian Government, Canberra, p. 79, http://www.pmc.gov.au/privacy/alrc_docs/stage1_aus_govt_response.doc [Accessed 29 November 2009].

the *Privacy Act* will be amended to clarify that, if an organisation transfers personal information to a related body corporate outside Australia or an external territory, the transfer will be subject to the 'Cross-border Data Flows' principle.[11]

Unfortunately, however, the proposed UPP 11 suffers from several of the same problems that privacy advocates have pointed to in NPP 9 for years. For example, the issue of focusing on "reasonable belief" and the issue of focusing on "substantially similar" protection remain the same. Further, while the ALRC sought to improve the consent requirement, for example, by stating that: "[a]ny bundled consent obtained should allow the individual to decide whether to consent to the cross-border transfer of their personal information",[12] it is not immediately clear how the issue of bundled consent will be dealt with on a practical level.[13]

5.1. OVERRELIANCE ON ACCOUNTABILITY

The most confronting issue in UPP 11 is its naive overreliance on accountability. Currently, UPP 11 requires the transfer to be based on one of a number of approved grounds, and where the transfer does not fall within either of those broad grounds, the agency or organisation responsible for the transfer will be accountable for how the personal information is treated by the recipient. This approach is seriously flawed. Where a transfer of personal information has no support in any of the wide circumstances outlined in UPP 11(a)-(f), there can be no justification for the transfer, even if some level of accountability applies to the agency or organisation responsible for the transfer. Such a transfer should quite simply not be allowed. In the change from NPP 9, to UPP 11, the Australian Government has gone from a weak regime aimed at preventing harm, to an unrealistic and naive hope of correcting harm after it occurs.

Several leading privacy experts have pointed to the flaws in the overreliance on 'accountability'. For example, Professor Greenleaf has observed that:

---

[11] Australian Government 2009, *First Stage Government Response to the ALRC Report 108*, Australian Government, Canberra, p. 79, http://www.pmc.gov.au/privacy/alrc_docs/stage1_aus_govt_response.doc [Accessed 29 November 2009].

[12] Australian Law Reform Commission 2008, *For Your Information: Australian Privacy Law and* Practice, Report No 108, Australian Government, Canberra, para. 1103.

[13] For a more detailed discussion of the consent issues, see Australian Law Reform Commission 2008, *For Your Information: Australian Privacy Law and* Practice, Report No 108, Australian Government, Canberra, Chapter 19. See also, Australian Government 2009, *First Stage Government Response to the ALRC Report 108*, Australian Government, Canberra, p. 38, http://www.pmc.gov.au/privacy/alrc_docs/stage1_aus_govt_response.doc [Accessed 29 November 2009].

> *The supposed virtue of the new approach is that although your personal information can be exported to anywhere that does not have 'substantially similar' privacy protections to Australia, if the exporter does so then theoretically they 'remain accountable' for overseas misuses of your personal information. 'Theoretical' is the key word, because the onus of proof (on the civil balance of probabilities) of a specific breach of a privacy principles by a specific overseas party still rests with you; as does the requirement to prove that the party in breach received the information directly or indirectly (but foreseeably) from the Australian exporting party; as does the requirement to prove that there was a causal connection between that breach and damage to you. And of course the country from which the damage to you emanated might not be the same as the country to which the data was exported, but you are the one who has to join the dots.*
>
> *How do you satisfy these requirements of proof when your data has travelled to Nigeria, India, Russia, the USA or 'all of the above', and you may not even know? Might it be dangerous to try? Might it be expensive?*
>
> *The so-called 'accountability' principle is a sham: the absence of any real likelihood of accountability is what is rotten at the core of the ALRC and Rudd Government approach.*[14]

In addition, commenting on the ALRC proposal, Connolly concluded that "[o]verall, the proposed UPP 11 is the weakest possible implementation of the accountability principle, and will do little to increase confidence in this new approach to privacy protection."[15]

The accountability approach should work as an added layer of protection – not as an alternative. Suggestions that accountability can replace the limitations to when transfer can take place, or that the limitations to when transfer can take place makes accountability unnecessary are misguided. To use an analogy, the fact that we have torts law does not mean we do not need traffic rules, and the fact that we have traffic rules does not mean we do not need torts law. Similarly, we need both limitations on when transfer can take place, and accountability rules for when transfer takes place.

Furthermore, any inclusion of an accountability scheme makes necessary rules governing the burden of proof. As pointed out above, the data subject will typically always be in a weak position in seeking to prove a breach –

---

[14] Greenleaf, G. 2009, 'Rudd Government abandons border security of privacy', *Australian Policy Online*, http://www.apo.org.au/commentary/rudd-government-abandons-border-security-privacy [Accessed 29 November 2009].

[15] Connolly, C. 2008, 'Weak protection for offshore data – the ALRC recommendations for Cross Border Transfers', *Galexia*, http://www.galexia.com/public/research/articles/research_articles-art54.html [Accessed 28 November 2009].

the data subject will experience the damages flowing from the breach, but may not be in a position to know where or how the breach occurred. This is particularly so, where the breach occurs overseas. Based on the above, it is submitted that where it is reasonable to assume that damages suffered by a data subject are due to a breach of the UPPs, the party held accountable under UPP 11 bears the burden of proving that no breach has occurred.

The appropriate starting point for UPP 11 is to outline the circumstances under which transfer is allowed. In doing so, the three categories established in the version of UPP 11 found in ALRC's Report 108 are useful (although some changes are required in the details). In addition to this, the agency or organisation responsible for the transfer should be accountable for the recipient's treatment of the personal information. In light of the above, it is submitted that UPP 11 ought to outline the circumstances under which transfer is allowed, as well as provide for accountability by the agency or organisation responsible for the transfer.

Despite introducing an accountability concept, UPP 11 still lacks adequate post-transfer accountability. That is because where export takes place within the very wide exceptions outlined in sub-sections a-f, the accountability requirement does not apply.

5.2. INTERNAL INVESTIGATIONS

On top of everything, the Government's response to the ALRC's recommendations manages to introduce an addition concern. The Government wants to add a sub-section to the effect that transfer can take place for the purpose of an internal investigation.

It is worrying to see that an organisation will be allowed to export personal information about Australian's based on that organisation having "reason to suspect" that unlawful activity or serious misconduct has been, or is being, or even may be, engaged in. It is not difficult to see how such a provision, for example, can be used to export personal data about Australians suspected of having played some role in illegal file sharing. While this paper does not aim to discuss the conflict between legitimate privacy concerns on the one hand, and copyright owners' legal right to find out who infringes their copy right on the other hand, it is submitted that allowing export as proposed will seriously undermine Australians' legitimate privacy expectations.

5.3. A BIT PREMATURE?

Finally, even leaving aside all the issues outlined here that need to be addressed for a successful UPP 11 to be put into place, it must be remembered

that the Australian Government is still to address several key aspects of the ALRC's recommendations in its second-stage report. Consequently, it is somewhat premature to finalise the structure for a UPP 11 – without knowing the exact scope within which UPP 11 is to operate,[16] it is simply not possible to finalise a text for UPP 11.

6. SOME OTHER KEY CHALLENGES

Any approach to the regulation of privacy in relation to transborder data flows on the Internet will be faced with severe challenges. Here, I discuss some of the key challenges such regulation must cope with.

6.1. CROSS-BORDER E-MAILS[17]

One fundamental problem of transborder data transfers arises in the context of e-mails containing personal information, being sent by, or to, e-mailing systems hosted overseas. This problem is augmented by the fact that, the laws of the place where the 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 the applicable privacy legislation in doing so? In answering this latter question, one 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

[16] It is, for example, not clear whether the current "small business" exemption will be kept.

[17] Parts of this sections draws upon: Svantesson, D. 2007, 'Protecting privacy on the "borderless" Internet – Some thoughts on extraterritoriality and transborder data flow', *Bond Law Review*, vol. 19, no. 1, pp. 168 – 187.

one doctor e-mailing the test results to another Australian doctor (an act that would be regulated by the 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 the applicable privacy law. 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. This is, however, likely to incur some costs for the organisations.

6.2. WEB PUBLICATIONS AND WEB 2.0

The Swedish *Lindqvist* case is an interesting example of the Internet-related issues that a provision dealing with cross-border data must be able to address. In that case, a woman – Bodil Lindqvist – who had taken a computer course uploaded a website on which she made available personal information about herself and her husband. The website also included personal information relating to a number of her colleagues in the church community she worked for. The information provided included matters such as full names, work duties, hobbies, family circumstances and phone numbers. She also discussed a foot injury suffered by one of the colleagues.

The website, which was published without the permission of her colleagues, generated some complaints and the matter ended up in court. While the legal proceedings related to a range of matter, such as whether Lindqvist's conduct amounted to "the processing of personal data wholly or partly by automatic means" for the purpose of the EU privacy directive[18], the interesting part for this paper is that the Court was asked to assess whether Lindqvist's conduct meant she had transferred the data in question to a third country. Göta hovrätt stayed the proceedings and referred seven

[18] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).

questions to the European Court of Justice (ECJ). Most interestingly, question five asked the ECJ to address the 'transfer' issue:

> *[Directive 95/46] prohibits the transfer of personal data to third countries in certain cases. If a person in Sweden uses a computer to load personal data onto a home page stored on a server in Sweden - with the result that personal data become accessible to people in third countries - does that constitute a transfer of data to a third country within the meaning of the directive? Would the answer be the same even if, as far as known, no one from the third country had in fact accessed the data or if the server in question was actually physically in a third country?*[19]

The Court answered this question in the negative.[20] However, it is interesting to examine how the Court reached that conclusion.

Having noted that "it is necessary to take account both of the technical nature of the operations thus carried out and of the purpose and structure of Chapter IV of that directive where Article 25 appears",[21] the Court made some observations as to the relevant technical setup:

> *It appears from the court file that, in order to obtain the information appearing on the internet pages on which Mrs Lindqvist had included information about her colleagues, an internet user would not only have to connect to the internet but also personally carry out the necessary actions to consult those pages. In other words, Mrs Lindqvist's internet pages did not contain the technical means to send that information automatically to people who did not intentionally seek access to those pages.*
>
> *It follows that, in circumstances such as those in the case in the main proceedings, personal data which appear on the computer of a person in a third country, coming from a person who has loaded them onto an internet site, were not directly transferred between those two people but through the computer infrastructure of the hosting provider where the page is stored.*[22]

---

[19] *Case C-101/01 Criminal Proceedings against Bodil Lindvist*, 6 November 2003, European Court of Justice, para. 18, http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=en&num=79968893C19010101&doc=T&ouvert=T&seance=ARRET [Accessed 24 November 2009].

[20] *Case C-101/01 Criminal Proceedings against Bodil Lindvist*, 6 November 2003, European Court of Justice, http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=en&num=79968893C19010101&doc=T&ouvert=T&seance=ARRET [Accessed 24 November 2009].

[21] *Case C-101/01 Criminal Proceedings against Bodil Lindvist*, 6 November 2003, European Court of Justice, para. 57, http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=en&num=79968893C19010101&doc=T&ouvert=T&seance=ARRET [Accessed 24 November 2009].

[22] *Case C-101/01 Criminal Proceedings against Bodil Lindvist*, 6 November 2003, European Court of Justice, paras. 60-61,http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=en&num=79968893C19010101&doc=T&ouvert=T&seance=ARRET [Accessed 24 November 2009].

While it is true that Lindqvist could not transfer the content of her website to an Internet user that was not connected to the Internet at the time, or who did not wish to take the steps necessary to visit her website, that is no different to the fact that a TV station cannot provide TV programs to somebody who does not turn on their TV, or who does not chose the TV station's particular channel. Consequently, the Court's justification of their approach, by reference to the relevant technology, is weak indeed.

The Court then turned to the purpose of the relevant part of the Directive:

> *Chapter IV of Directive 95/46 contains no provision concerning use of the internet. In particular, it does not lay down criteria for deciding whether operations carried out by hosting providers should be deemed to occur in the place of establishment of the service or at its business address or in the place where the computer or computers constituting the service's infrastructure are located.*
>
> *Given, first, the state of development of the internet at the time Directive 95/46 was drawn up and, second, the absence, in Chapter IV, of criteria applicable to use of the internet, one cannot presume that the Community legislature intended the expression 'transfer [of data] to a third country' to cover the loading, by an individual in Mrs Lindqvist's position, of data onto an internet page, even if those data are thereby made accessible to persons in third countries with the technical means to access them.*[23]

This conclusion is not justified. The fact that the Directive does not make specific mention of the Internet, suggests that it is drafted in technology neutral language. Where that is the case, it cannot be assumed that the drafters did not intend the Directive to apply to Internet related activities such as in the *Lindqvist* case. Rather, the technology neutral language suggests that the application of the Directive should not be dependent on the technology in question. The Courts conclusion is perhaps even more extraordinary when one considers that the Internet was in place (be as it may on a different scale) at the time the Directive was drafted. Consequently, had the drafters wanted to exclude Internet activities, they would presumably have made that clear.

The third justification the Court presented for their conclusion is more interesting:

---

[23] *Case C-101/01 Criminal Proceedings against Bodil Lindvist*, 6 November 2003, European Court of Justice, paras. 67-68, http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=en&num=79968893C19010101&doc=T&ouvert=T&seance=ARRET [Accessed 24 November 2009].

> *If Article 25 of Directive 95/46 were interpreted to mean that there is 'transfer [of data] to a third country' every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet. The special regime provided for by Chapter IV of the directive would thus necessarily become a regime of general application, as regards operations on the internet. Thus, if the Commission found, pursuant to Article 25(4) of Directive 95/46, that even one third country did not ensure adequate protection, the Member States would be obliged to prevent any personal data being placed on the internet.*[24]

This argument is much harder, if not impossible, to dismiss, and it shows a type of thinking that is far too rare amongst courts having to address legal issues associated with rapidly developing technologies. Instead of merely applying the law to the situation at hand, the Court made an assessment of the likely consequences of finding that Lindqvist's conduct amounted to transfer. In other words, while it may be difficult to argue that Lindqvist's conduct did not amount to a transfer, the consequences of reaching such a finding would be devastating for the technology in question – a reasonableness test was applied.

In this context, it is interesting to note the ALRC's statement that:

> *Generally, if personal information is stored in Australia, but is accessed or viewed outside Australia, it should be considered to have been transferred. If personal information is routed and temporarily stored outside Australia, but is not accessed, it should not fall within the purview of the 'Cross-border Data Flows' principle. If it is accessed, however, it should be subject to the principle.*[25]

In light of this remark, it is possible that a situation such as that in the *Lindqvist* case would have been viewed as amounting to transfer under Australian law.

If the situation is complicated in the context of publication of personal information on websites, it gets even worse if we consider more recent technologies. Imagine, for example, that instead of placing the relevant information on a website, Bodil Lindqvist would have placed the same information on her Facebook site. Imagine further that she was aware that some of her

---

[24] *Case C-101/01 Criminal Proceedings against Bodil Lindvist*, 6 November 2003, European Court of Justice, para. 69, http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=en&num=79968893C19010101&doc=T&ouvert=T&seance=ARRET [Accessed 24 November 2009].

[25] Australian Law Reform Commission 2008, *For Your Information: Australian Privacy Law and* Practice, Report No 108, Australian Government, Canberra, paras. 1116-1117.

Facebook "friends" were located in countries outside the European Union. In such a situation, it would be much easier to argue that she intentionally transferred the data to another country. However, bearing in mind the nature of Facebook, the consequences of finding the conduct to amount to "transfer" would be much the same as finding that Bodil Linqvist transferred the data to another country by placing it on her website – it would mean that one simply could not place personal information relating to another person on one's Facebook site in the event that one has "friends" in another country.

6.3. CLOUD COMPUTING[26]

Cloud computing is a vague term typically used to refer to a technical arrangement under which users store their data on remote servers under the control of other parties, and rely on software applications stored and perhaps executed elsewhere, rather than on their own computers. The term encompasses a variety of services, which are variously of long standing (including email[27]), long-promised (including 'software as a service'), and relatively new.

There are many potential benefits with such arrangements. For example:

- The user can access the same set of applications, and the same data, regardless of location, and regardless of which hardware they use (such as computers, PDAs and mobile phones, including both their own hardware and devices borrowed from other individuals and organisations);
- Several users can access and share the same applications and data which assists in collaborative work;
- Backup and recovery is delegated to a service-provider, which presumably enhances its reliability;
- Licensing of software and third-party data can be simplified; and
- Complex tasks can be performed by using less powerful devices by depending on more powerful remote servers.

At the same time, cloud computing is associated with severe risks in the areas of service and data integrity, consumer rights, security and privacy.

[26] Parts of this sections draws upon: a policy statement drafted for, and together with other members of, the Australian Privacy Foundation 2009, *APF Policy Statement re Cloud Computing* http://www.privacy.org.au/Papers/CloudComp-0911.html [Accessed 29 November 2009].

[27] In that sense, a discussion of the problems associated with cloud computing has already taken place in the discussion of hotmail above. However, as the e-mail situation could arise outside the scope of cloud computing, and as cloud computing issues go beyond the situation discussed, I have chosen to discuss cloud computing as a separate issue.

Most importantly, for the discussion in this paper, cloud computing fits very uneasily with the idea of transborder data flow regulation. In fact, in the typical cloud computing situation, the location of the data is irrelevant and is often unknown to the user of the cloud-computing service, and possibly even to the supplier. In light of that, it seems unlikely that the user could be adequately informed to give valid consent to the transfer.

7. RECOMMENDATION

As already noted, it is not possible to draft UPP 11 until a range of matters, such as the exact scope of the *Privacy Act*, has been established. However, having taken account of the above, I propose that Australia adopts a provision governing cross-border data, along the following lines:

> *11.1 An agency or organisation[28] shall not transfer personal information to a recipient (other than the agency, organisation or the data subject) who is outside Australia and an external territory unless:*
>
> *(a) the recipient of the information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to, or more favourable to the data subject than, this Act and which are enforceable by the data subject;*
>
> *(b) the data subject consents to the transfer, after being expressly advised of the country or countries which are the destination(s) of the transfer, the intended recipient(s), the protective measures that will be taken in relation to the personal information, how the personal information will be used at the destination, and whether the personal information will be transferred from the destination country (where the personal information will be transferred from the destination to a third country, all the information outlined here must also be provided in relation to the third country); or*
>
> *(c) the agency or organisation is required by Australian law to transfer the personal information to the recipient.*
>
> *11.2 Where an agency or organisation transfers personal information to a recipient (other than the agency, organisation or the data subject) who is outside Australia and an external territory, it remains strictly liable for how*

[28] Unlike the other UPPs, UPP 11 includes a jurisdictional limitation in that it is limited to the conduct of an agency or organisation "in Australia or an external territory". First, from a structural perspective, the jurisdictional scope of the UPPs ought to be uniform. There is no reason to have different standards for different UPPs. Indeed, such differences complicate the application of the UPPs in an unnecessary manner. Second, and more seriously, limiting UPP 11 to agencies and organisations in Australia or the external territories opens the door for agencies and organisations, based overseas, transferring overseas data without any regard for the protection that UPP 11 ought to provide. Consequently, it I have opted to remove the limitation to an agencies and organisations "in Australia or an external territory".

the personal information is used by the recipient, unless the transfer falls within 11.1(c).

11.3 After appropriate consultation, the Government shall produce and maintain a list of jurisdictions deemed to have laws and/or binding schemes that satisfy the requirement of 11.1(a).

11.4 After appropriate consultation, the Government shall produce and maintain a list of standard clauses that must be included in contracts of the type envisaged in 11.1(a).

11.5 Consent as described in 11.1(b) must not be bundled.

8. CONCLUDING REMARKS

Some commentators view the European Court of Justice's decision in the *Lindqvist* case as "draconian and abusive"[29] and have pointed to that case as an illustration that US lawmakers must steer clear of EU-style "heavy-handed centralized legislation".[30] They suggest that the better approach is to focus on whether any damage has been caused: "An action such as this [i.e. the Lindqvist case] would be highly unlikely in the United States without at least the perception of harm by some party. In the United States, the party perceiving harm would seek to remedy that harm, generally as an individual with an equity or tort claim."[31]

Not only does this illuminate a deep-seated difference in attitude between Europe and the United States, it also brings attention to a fundamental choice facing countries like Australia that are structuring or re-structuring their privacy regulation. On the one hand there is the option of a European-style regulation aimed at preventing harm, and on the other hand there is the option of a US-style regulation mainly aimed at compensating where harm occurs.

I think a comparison with traffic regulation can be illustrative also in this high-level context. We have rules about how fast cars can travel on our roads. While most people would have felt frustration on some occasion in having to drive slower than the conditions may warrant, we realise that the speed rules are in place to avoid harm. We recognise that it is better to try to

---

[29] Garcia, F. J. 2005, 'Bodil Lidnqvist: A Swedish Churchgoer's Violation of the European Union's Data Protection Directive Should Be a Warning to U.S. Legislators', *Fordham Intellectual Property, Media & Entertainment Law Journal*, vol. XV, p. 1233.

[30] Garcia, F. J. 2005, 'Bodil Lidnqvist: A Swedish Churchgoer's Violation of the European Union's Data Protection Directive Should Be a Warning to U.S. Legislators', *Fordham Intellectual Property, Media & Entertainment Law Journal*, vol. XV, p. 1233.

[31] Garcia, F. J. 2005, 'Bodil Lidnqvist: A Swedish Churchgoer's Violation of the European Union's Data Protection Directive Should Be a Warning to U.S. Legislators', *Fordham Intellectual Property, Media & Entertainment Law Journal,* vol. XV, p. 1229.

avoid traffic-related harm being suffered, than it is to compensate for such harm. In light of that, we conclude that a person may be penalised for speeding even where the speeding does not cause any harm – speeding is the regulated activity, not just the causing of harm through speeding.

Applying this thinking to privacy regulation, we may have to accept that privacy laws may feel restrictive in some cases, but they are there to avoid harm being suffered through misuse of our personal information. Thus, we need to make sure that a violation of our privacy rights is taken seriously even where we cannot point to any specific harm being suffered as a consequence of that violation.

Having said that, as I have pointed out above, the appropriate way forward, at least as far as cross-border data flows are concerned, is to combine the EU-style focus on preventative regulation (through border control) with the US-style focus on compensation for harm (through the application of the accountability principle).