# The APEC Asia-Pacific Privacy Initiative – a new route to effective data protection or a trojan horse for self-regulation?

Nigel Waters Pacific Privacy Consulting Australia

June 2008

Privacy Laws and Business 21st Annual International Conference,
8 July 2008, Cambridge, England[1]

## Table of Contents



This paper is written from multiple perspectives – the author has an interest in the APEC privacy initiative as a consultant[2], as an academic[3] and as a privacy and consumer advocate[4]. He has been a member of the Australian delegation to meetings of the APEC Data Privacy Sub-group since 2007, and also represented Privacy International[5] at the most recent meetings in Lima, Peru, in February 2008. Nigel Waters is a former Australian Deputy Privacy Commissioner (1989-1997), and Assistant UK Data Protection Registrar (1985-89).

The author thanks Professor Graham Greenleaf and Mr Colin Minihan, Chair of the APEC Privacy Subgroup, for their helpful comments on drafts of this paper.



1 See http://www.privacylaws.com
2 Pacific Privacy Consulting, since 1997 http://www.pacificprivacy.com.au/
3 Research Fellow and principal researcher on the Interpreting Privacy Principles project at the Cyberspace Law and Policy Centre, University of New South Wales, Australia. http://www.cyberlawcentre.org/ipp/
4 Board member of the Australian Privacy Foundation http://www.privacy.org.au and of the Consumers Federation of Australia http://www.consumersfederation.org.au/
5 http://www.privacyinternational.org

## Background

Asia Pacific Economic Cooperation (APEC) is a grouping of 21 member economies in the Asia Pacific Region which between them account for more than 40% of world population and 50% of world GDP (including Russia, China and the United States). It was established in 1989 to facilitate economic growth, cooperation, trade and investment in the region.

The APEC Privacy Framework was adopted by Ministerial Declaration in October 2004, after a two year development by a Privacy Subgroup of the APEC Electronic Commerce Steering Group (ECSG)[6], with the Implementation section added a year later. The Subgroup has continued to meet regularly to progress implementation of the Framework. The current emphasis is on a number of linked Pathfinder projects, in one of more of which 14 of the 21 APEC member economies are currently participating.

Relevant papers can be found on the APEC website[7]

## Different Perceptions

There has so far been relatively little independent critical analysis of the APEC Privacy Framework. Opinion is divided as to whether the APEC initiative is a positive or harmful development.

At one extreme, Chris Pounder of Pinsent Mason and editor of Data Protection Quarterly has stated that:

> *"The lack of detail in the Framework makes it a shaky foundation that risks creating national privacy laws and rules that would be inconsistent with each other and far weaker than Europe's traditional approach to the subject."* [8]

A more positive view has been put by Johanna Tan from Singapore. She argues that:

> *"... perhaps the APEC Privacy Framework is the first step towards a truly global standard for data protection."*[9]

although she also sees the Framework as having a more limited objective, focussed on economic aspects of global trade.[10]

Professor Graham Greenleaf of the University of New South Wales has been following the development of the Framework since its inception. His most recent assessment lies between those of Pounder and Tan:

---

6 The Subgroup was formed in response to an Australian government proposal 'An APEC Approach to Privacy Protection – Paper 2003/SOM/ECSG/003 for the ECSG meeting in Thailand, February 2003

7 At http://www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce.html with detailed papers at http://aimp.apec.org/MDDB/pages/BrowseMeeting.aspx – it is necessary to know the date of the meetings in order to find the relevant papers – recent meetings were in February 2008 (Lima), June 2007 (Cairns) and January 2007 (Canberra).

8 Pounder C [2007] Why the APEC Privacy Framework is unlikely to protect privacy. Online at http://www.out-law.com/default.aspx?page=8550

9 Tan J [2008] A Comparative Study of the APEC Privacy Framework- A New Voice in the Data Protection Dialogue? Asian Journal of Comparative Law *Volume* 3, *Issue* 1 2008 *Article* 7, abstract

10 Tan, ibid, page 23.

*"[the APEC Framework's] Privacy Principles set the lowest standards of any international privacy agreement; and it has no meaningful enforcement requirements." but he also sees that:"...it could still play a useful role in the gradual development of higher privacy standards in Asia, provided its priorities are re-oriented."*[11]

In my view, both Pounder and Greenleaf are somewhat harsh in their assessment of the APEC principles (as opposed to the overall Framework, including implementation and enforcement aspects), while Tan is too uncritical.

That some stakeholders will seek to use the APEC Framework to counter other initiatives which they see as more threatening[12] is not surprising, but this should not mean that we suspend judgement of the Framework on its merits.

## How do the APEC Principles measure up?

The APEC Framework includes some definitions and a set of Principles[13], which depart somewhat from the familiar 'data life cycle' approach taken by other instruments and laws, but cover similar ground. The next section of this paper focuses on those principles which have attracted particular controversy – the others, which deal with data integrity (quality), security and access and correction, are relatively uncontroversial and are not addressed here.

Both Pounder and Greenleaf are suspicious of the elevation of a 'harm' test to the status of a principle[14]. They fear that the statement in the Principle that 'specific obligations should take account of such risk [of harm].' will be interpreted as a threshold test for other rights or obligations. Tan's assessment that the 'preventing harm' principle is a conscious differentiation of the APEC framework as a pragmatic facilitator of e-commerce, in contrast to a 'rights based' European model[15], is somewhat provocative and re-inforces other commentators' suspicions. But the commentary on this principle does not provide any support for the fear. The statement about risk can be seen as no different from the 'such steps as are reasonable in the circumstances' qualifier found in many principles in most laws, which allow data users to base their compliance on their own risk assessment – subject to independent judgement in case of complaints or audits. In Subgroup discussions, assurances have been given that it is not intended to interpret the harm principle as meaning that a breach is only significant if there is economic loss[16]. There will hopefully be little argument that harm – including emotional distress – should be a relevant factor in relation to enforcement priorities and remedies.

---

11 Greenleaf G [2008], Five years of the APEC Privacy Framework: Failure or promise? Presented at the ASLI conference (forthcoming publication at http://law.bepress.com/ )

12 As Google's Global Privacy Counsel appears to have been doing in statements in September 2007

13 APEC Privacy Framework, Parts II (Scope) and III (Principles) respectively

14 Principle I in the APEC Framework is 'Preventing Harm'

15 Tan, ibid, page 20

16 Unlike in the New Zealand law, which undermines the effect of the principles by inserting a harm test in the grounds for complaint – see Privacy Act 1993 [NZ] section 66(1)(b).

The notice principle in the APEC Framework[17] has been criticised for allowing too much discretion as to the timing and content of notices. In particular, Pounder points to the express allowance for giving notice 'after' the time of collection. However, the EU Directive notice obligation for direct collection[18] is silent as to timing, the OECD purpose specification principle[19], while unambiguous as to timing, does not expressly require notice *to the individual*, and the CoE Principles do not even include a requirement for proactive notice. Arguably the APEC Notice principle and accompanying commentary simply recognise openly the practical constraints on notification, which in other regimes are accommodated by a combination of guidelines and non-enforcement of unrealistic absolute standards. Greenleaf concludes that the APEC notice principle is stronger than the OECD equivalent.

Some of the privacy principles cannot sensibly be compared in isolation from each other, as it is often the way in which two or more principles interact that determine the strength or weakness of their effect. This is particularly the case with those principles that deal with use and disclosure, and with individual choice or participation.

Pounder points out that the APEC Use principle[20] allows for 'compatible *or* related purposes, without consent (my emphasis), and Greenleaf fears that the other exception – where 'necessary to provide a [requested] service or product' is open to abuse. The OECD's use limitation principle allows use in only three circumstances – for another specified purpose which is not incompatible (with the purposes specified at collection), with consent and by the authority of law. The EU Directive allows for use in six circumstances[21], including with 'unambiguous consent' – a strict test – but also 'in the public interest' and in the 'legitimate interests' (of the controller or a third party) – both of which are open to very broad interpretation. The Council of Europe Convention provides for compatible uses[22], but has no role for individual choice or consent.

Of course, both 'compatible' and 'related' are also open to interpretation, and it cannot be assumed that the former is necessarily a stricter constraint than the latter, or vice versa.[23] Similarly, 'consent' is a very elastic concept which few instruments or laws define adequately to protect against self-serving interpretations such as where provision of consent is made a condition of a transaction[24], and often by all providers so that an individual has no alternative. The inclusion of 'unambiguous' in the EU principle sets only one of the tests which would be necessary to establish a genuine consent – which would also need to be freely given, fully informed and revocable. As Greenleaf notes,

17 Principle II in the APEC Framework is 'Notice'.
18 Directive EC95/46 Article 10
19 OECD Guidelines 1980, Part 2, Principle 9
20 Principle IV in the APEC Framework is 'Use'
21 Directive EC95/46 Article 7
22 Convention 108, Chapter 2, Article 5(b)
23 Pounder assumes that APEC means the terms 'compatible' and 'related' to mean something different. The commentary makes no attempt to distinguish the two with examples, and I suggest that it is just as likely that they were both included as alternative descriptors – this often occurs even in laws which have been subject to professional legislative drafting, which the APEC Framework has not
24 As illustrated by Pounder in his discussion of the APEC Choice principle, but applicable to all 'consent' based principles – Greenleaf also refers to the problem of 'bundled' consent.

the second exception to the APEC Use principle is similarly open to self-serving interpretations.

The EU Directive provides for a right of objection to some uses, expressly including an free opt-out from direct marketing,[25] but the OECD Individual Participation principle[26] and the equivalent provisions in the COE Convention[27] grant only a right to challenge data users for breaching other principles – they do not give individuals any say over uses or disclosures.

Taking the limits on uses and disclosures overall, it is not clear that the APEC Principles are any weaker than the other international instruments. If an underlying objective of any information privacy instrument is to empower individuals, then by requiring the provision of choice 'where appropriate'[28], APEC arguably[29] sets a *higher* standard, although as always, whether it is effective depends on domestic implementation.

APEC Principle IX – Accountability – mirrors the similar principle 14 in the OECD Guidelines. Greenleaf is concerned about its application only to data controllers and not their agents, but this appears to be a deliberate design feature in the Framework, which seeks to lay responsibility unambiguously with the entity with whom an individual enters a direct relationship. This is a good feature in that it avoids 'buck-passing', but will clearly only be effective if the principles can be enforced against the data controllers. The Accountability principle also requires due diligence by controllers when transferring personal information to a third party, to take reasonable steps to ensure that it will continue to be protected consistently with the APEC Principles.[30]

Tan seeks to differentiate this APEC principle from the approach of the other international instruments to transborder data flows – in her view the emphasis on continue accountability for 'exported' data is an alternative to the 'transfer prohibition' approach, best exemplified by the EU Directive[31]. But this overlooks the intended role of prohibitions, not only in the Directive[32] but also in the COE Convention[33] and OECD Guidelines[34] – prohibition is not an end in itself but as an exceptional sanction to avoid the circumvention of privacy protection by transferring data across borders. The provisions are also expressly designed, in the context of the instruments overall, as an incentive for enhanced privacy protection so that information can be transferred.

25 Directive EC95/46 Article 14
26 Guidelines Part 2 Principle13
27 Convention 108, Article 8
28 Principle V in the APEC Framework is 'Choice'
29 The effect of the Choice principle maybe undermined by the unfortunate wording of the Collection Limitation Principle (Principle III) which sets up 'notice to' and 'consent of' as alternatives. However, as in other areas of drafting it not clear that APEC intended to make this distinction.
30 Principle IX, paragraph 26
31 Tan, ibid, page 21
32 Directive EC95/46 Articles 25&26
33 Convention 108, Article 12
34 Guidelines part 3, paragraph 17

As Greenleaf rightly points out, Principle IX is a 'soft substitute for a Data Export Limitation principle' which potentially leaves individuals without any recourse where a recipient of data breaches the principles despite the best endeavours of the disclosing organisation. However, the APEC Privacy Subgroup has acknowledged this problem and is seeking to address it in the Pathfinder projects described below. Emphasis on a data exporter remaining accountable for compliance is at the heart of the Cross Border Privacy Rules approach, and the limitations of enforcement remain an issue for all data protection regimes, not just the APEC Framework.

The APEC approach to cross border transfers is different from that taken by the other instruments, in that it does not seek to guarantee free flow of personal information provided certain conditions are met. However, taken in the context of the Implementation provisions of the Framework and of the developing work on the Pathfinder projects, the APEC accountability principle is heading in the same direction as initiatives under those instruments. Specifically, the Cross Border Privacy Rules work under the APEC Pathfinder has much in common with the Binding Corporate Rules work in relation to the EU Directive. The main difference would appear to be that some stakeholders clearly perceive the BCR work as having stalled in a morass of inconsistent interpretations by European regulators[35], with the APEC CBPR initiative offering a fresh start on essentially the same mission.

Commentators have also taken issue with some aspects of the Scope part (Part II) of the Framework which determines the applicability of the principles. Pounder is critical of the treatment of 'publicly available information' in the APEC Framework. These provisions[36] are ambiguous. Publicly available information is not 'exempt' – the commentary on the definition suggests that some of the principles may have only limited application to publicly available information, and specifically suggests that this will be the case with journalistic output, and where information is required by law to be made public. However, most privacy or data protection laws have some exemptions for publicly available information, for journalism and for actions 'required or authorised by law.' By merely qualifying rather than exempting 'publicly available information' the APEC Framework arguably leaves it covered better by the principles than it is in many other regimes.[37]

Greenleaf comments on the 'Application' section of Part II, which provides for exceptions to the Principles, which should however be limited and proportional and either made known to the public or in accordance with law[38]. Greenleaf suggests that the 'or' in this last provision is probably a mistake and should be 'and' as otherwise it would allow organisations to write their own exemptions. But the commentary to this paragraph makes it clear that it is addressing the circumstances in which member economies would

35 See also criticisms by Bygrave L [2002], *Data Protection Law: Approaching its Rationale, Logic and Limits*, Aspen Publishers Inc, cited by Tan, ibid, page 30

36 Part II of the Framework – paragraph 11

37 For example, the Australian Privacy Act expressly excludes 'generally available publications' from the definition of 'record', and most of the principles apply only to records.

38 Paragraph 13

allow exemptions, rather than a issuing a direct invitation to affected data users, so the consequence of the drafting error can hopefully be corrected in implementation.

There are some clear deficiencies in the APEC Principles, pointed out by Pounder - such as the absence of an express data retention or disposal principle[39], and the breadth of the exemptions from the right of access, although in the latter case, similar exemptions could be provided in domestic law under all of other main instruments - the EU Directive[40], the COE Convention[41], and the OECD Guidelines[42].

In summary, the APEC principles themselves, despite some deficiencies, are not too bad as a 'floor', and arguably little different in one key respect from the OECD Principles, the EU Directive Articles or the COE Convention 108 Principles in that all allow for considerable interpretation when they are translated into binding obligations. Pounder suggests that the EU Directive was a response to the Convention being too general and 'high level' and that the APEC Framework runs the risk of being similarly too general. I suggest that the EU Directive, while appearing to be more specific in some respects, is substantively just as subject to differing interpretation as the other instruments. High level principles in international instruments will inevitably be pitched at the level of general principles which are a product of compromise and to some extent a 'lowest common standard'.

Of greater practical significance is the way in which the obligations are firstly embodied in domestic law and secondly enforced.

## How will the APEC implementation scheme work?

In the two years after adoption of the Framework, the Subgroup's main focus was on building capacity and understanding of the issues in member economies. The original Framework adopted in 2004 was a work-in-progress in relation to Implementation, and it was not until September 2005 that the Part IV – Implementation – was added to the Framework.

Part IV clearly envisages domestic regulation, including legislation, as an option for implementation of the Framework[43]. There is also encouragement for the preparation of individual action plans by each economy, to report on progress in domestic implementation.[44] While some members are understood to have prepared action plans, bureaucratic obstacles have prevented their publication, so it is difficult to tell what progress is being made overall. Delegation reports to the Subgroup meetings have however indicated that several economies are considering legislative options. Peru,

39 Although this author has previously argued that a requirement to dispose of information once it is no longer required can be inferred from both data quality and data security principles – see Waters, N. and Greenleaf, G. 2006, 'Interpreting Retention and Disposal Principles, v.1', Interpreting Privacy Principles Project, University of New South Wales

40 Directive EC95/46 Article 13

41 Convention 108, Article 9(2)

42 Guidelines Part 1 paragraph 4

43 Part IV.A.II of the Framework – paragraph 31

44 Part IV.A.VI of the Framework

China, Thailand, Viet Nam and the Philippines all reported in Lima in February 2008 that they are moving ahead with the introduction of information privacy laws (although none of them, paradoxically, appear to be paying too much attention to the APEC Principles in their design). In fact, it appears that *lack* of data protection laws is perceived by some members as a trade barrier – e.g. Peru has put data protection law, based on the European model, on the fast track in order to attract more Spanish language call centre operations to service other countries.

Since late 2006, the Subgroup's focus has moved onto the development of Cross Border Privacy Rules (CBPR) mechanisms and processes, which are expressly encouraged by the implementation guidance in the Framework (Part IV.B.III).

After some initial uncertainty, it has become clearer that the practical implementation of the CBPR approach is intended to be as follows:

- A business seeking to participate will prepare a document setting out how it will comply with any applicable standards, and how it will deal with any complaints about breaches; i.e. a version of the privacy policy or privacy statements which are required by some domestic laws (and by APEC principle II). This self-assessment will be based on a standard set of questions.

- A business' self-assement document would be assessed by an 'accountability agent' (which might be a regulatory agency or a 'trustmark' organisation) against a set of criteria.

- Accountability agents would be approved based on a separate assessment process, for which guidelines and criteria will also be developed.

- If assessed as meeting the requirements, the business would be included in a publicly accessible directory of compliant organisations.

- Regulators will establish mechanisms for cooperation on complaints that involve multiple jurisdictions, and on cross border enforcement. This cooperation may involve accountability agents other than regulators.

## Progress on the Pathfinder projects

Work on the Pathfinder projects, approved in 2007 as the basis for further work on the CBPR approach, has intensified since the February 2008 Subgroup meeting.[45] A series of telephone/internet conferences have been held for each of the three main 'groups' of projects, as follows:

**Self assessment** (Project 1) – led by the ICC **and Compliance review processes** (Project 3) – led by the United States. Progress on these projects has been hindered by a 'stalemate' in which business wanted regulators to specify their requirements first, while

45 See the 'APEC Data Privacy Pathfinder Projects Implementation Work Plan' document that was endorsed for public release at the February 2008 meeting

regulators wanted business to make the first move. This has now been broken with a recognition that the two projects need to be progressed in parallel, as they depend so much on each other. Joint teleconfonferences are now being held.

**Guidelines for accountability agents** (Project 2) – led by the United States. While the initial work has focussed on private sector accountability agents such as 'trustmark' or 'seal' programs, it has been recognised that recognition criteria will also be required for government agencies in those countries where they will be the accountability agents, and that common criteria are therefore desirable.

**Cross border enforcement cooperation** (Projects 5, 6 & 7) – led by the Office of the Privacy Commissioner (OPC), Australia. Useful progress has been made on directories of contacts, agreements between regulators and templates for referral of complaints. The parallel work of the OECD's Working Party on Security and Privacy on cross border enforcement[46] has been recognised and there is an attempt to harmonise processes.

Pathfinder project 9 will seek to test the entire process, starting with a number of volunteer businesses submitting self-assessment results documents for 'processing' by accountability agents. The complaints and enforcement mechanisms being developed in projects 6 & 7 will then be tested on hypothetical 'breach' scenarios. The overall 'test' (Project 9) will not formally commence until after the August Subgroup meeting, but is already being kept in mind by participants in the other projects.

An important element currently missing from the Pathfinder is the mechanism by which the regulator in any one jurisdiction, or collectively, would assess the credentials of the 'accountability agent' in another jurisdiction. Project 2 will deliver assessment criteria for agents, but who will make the decision that a particular trustmark scheme or regulatory agency meets these criteria? And as with the organisational self-assessments, the issue of public transparency arises.

It has always been recognised that additional projects may be necessary, and that in any event the Sub-Group has the overall responsibility for resolving issues that fall outside the individual projects (these points are explicitly stated in the Work Plan. Australia remains chair of the Subgroup, and convenes regular Subgroup teleconferences, most recently in May to coordinate the Pathfinder work and to plan for the next meeting, and technical assistance seminar, again in Lima, Peru, in August 2008.

There is recognition of the need for better communications, transparency and 'outreach' about the APEC initiative, and a 'friends of the chair' group has been formed to address these issues. It is recognised that there are some semantic obstacles to understanding, even amongst native English speakers, let alone those with other first languages. Consideration is being given to finding an alternative to the term 'Cross Border Privacy Rules (CBPR)' as this implies yet another set of substantive standards, whereas the main

46 OECD [2007] Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy - developed by the OECD Committee for Information, Computer and Communications Policy (ICCP), through its Working Party on Information Security and Privacy (WPISP).

focus of the work is on mechanisms and infrastructure for the effective implementation of existing privacy 'rules' with the APEC principles as the minimum 'floor'. The fact that CBPR is is used in the adopted Framework probably means that it cannot now be abandoned, but it would be helfpul to use alternative terms in any public presentations.

## Stakeholder imbalance and Civil Society input

It needs to be recognised that APEC's focus is much narrower than that of either the EU or the Council of Europe, and narrower even than the OECD which shares APEC's terminological focus on economic matters. Unlike the other forums, APEC has few strands of work that are outside the economic, commercial and trade areas. And unlike in those forums, Civil Society is not recognised as a formal partner by APEC. Civil Society has only been represented in the APEC Privacy processes by virtue of invitations from specific member economies to be part of their delegations. However this effectively means only observer status. This contrasts with formal recognition of business interests – both the International Chamber of Commerce and the Global Business Dialogue on e-Commerce have guest status at the Privacy Subgroup, with independent participation rights. It should be noted that privacy regulators are recognised as important stakeholders, although their contribution to the work of the APEC Privacy Subgroup has been limited by resource constraints – international cooperation and participation in international privacy developments are typically not high on the priority lists of small under-resourced privacy protection authorities.

Partly in response to persistent criticism of stakeholder imbalance, APEC has publicly acknowledged[47] the need for Civil Society input to its privacy work. This unusual but welcome departure from APEC norms can probably be attributed to a recognition of the importance of building consumer trust and confidence in electronc transactions and cross-border data transfers if the wider trade and development objectives of APEC are to be met.

Civil Society representatives, including this author, have contributed to the technical assistance seminars preceding Subgroup meetings, and both Privacy International and the Electronic Privacy Information Centre (EPIC) made presentations to the Subgroup in support of their applications for independent 'guest' status.

While a recommendation to accept went forward from the Subgroup to the 'parent' ECSG, one economy is understood to have raised concerns, and because APEC operates on a consensus basis, further consideration was deferred to allow the Chair to gather further information to respond to the concerns.

Even without formal guest status, Civil Society representatives have been invited to participate in the telephone conferences progressing the Pathfinder projects and have done so on some occasions. While this invitation has provided opportunities for Civil Society to influence the implementation of the APEC Framework, resource limitations are a significant constraint. If APEC is serious about consultation with Civil Society, it

47 Including in the Ministerial statement from the September 2007 APEC 'summit' in Sydney.

needs to address the question of funding for continued participation by informed consumer and privacy advocates in the APEC processes.

Civil Society input has focussed on some of the deficiencies in the Framework including those identified by Pounder and Greenleaf. Civil Society representatives have continued to express a strong preference for national data protection legislation with higher standards and effective enforcement mechanisms, to ensure accountability and compliance, as the simplest and least cost route both for consumers and for business.

Civil Society also resists suggestions, made periodically[48], that the APEC Framework is partially a response to significant cultural differences and differing interpretations of privacy. The Framework does expressly recognise a 'wide range of different social, cultural and economic and legal backgrounds of member economies'[49], but this should not be used as basis for weakening accepted principles. Privacy is widely recognised as a universal and fundamental human right[50], and common information privacy principles have been successfully adopted by cultures as diverse as those in Korea, Japan, Taiwan, Hong Kong, Australasia and Latin America as well as throughout Europe with all its internal diversity, especially after recent expansion. Civil Society can see no foundation for arguments that existing international privacy instruments are culturally specific and therefore inappropriate as a model for some countries.

Within the Pathfinder, Civil Society argues for priority to be given to the cross-border enforcement mechanisms which are equally relevant to legislative schemes and the CBPR approach.

## Relationship to other international privacy instruments

It seems clear that the initial stimulus for the APEC Framework was a desire to provide an alternative to the influence of the EU Data Protection Directive, and to 'head off ' any potential prohibitions on cross border data transfers either by EU member states or by those regional jurisdictions which have incorporated EU-style trans-border privacy rules into their domestic legislation (such as Australia[51] and Hong Kong[52]).

But as I have argued above, the potential for the APEC Framework to provide a 'softer' option with lower hurdles to be jumped to allow cross border data transfers has not and cannot be realised, and it now appears to be simply an alternative route to the same goal – of a system for allowing international flows of personal information without sacrificing privacy protection. There are too many 'lines in the sand' drawn by the domestic laws of key trading countries to allow either the APEC initiative or any other developments to undermine existing privacy protection standards. For this to occur, laws in Europe, Australia, Hong Kong, and possibly soon in other APEC countries mentioned above as

48 Including by several speakers at the APEC Technical Assistance Seminar in Lima in February 2008
49 APEC Framework, Part II, Paragraph 12
50 Including in the Universal Declaration of Human Rights (Article 12) and the International Covenant on Civil and Political Rights (Article 17)
51 Privacy Act 1988, Schedule 3, National Privacy Principle 9
52 Personal Data (Privacy) Ordinance 1995 s.33 (although this section is not yet in operation)

bringing forward legislation, would need to be amended to weaken their limits on cross border transfers. This is not in prospect in any country[53], and seems unlikely.

If the APEC Framework is to achieve its objective of removing barriers to the cross border flows of personal information, there is no escaping from the need, ultimately, for an 'adequacy assessment' mechanism similar to the EU Directive's Article 29 & 31 Committee processes. No economy, and in particular no regulator in those economies with a legislated cross border transfer principle (currently only Australia and Hong Kong amongst APEC members) will ultimately be able to avoid making a decision about which other jurisdictions meet their required minimum standards - both of substantive rules/principles, and of compliance and enforcement mechanisms. In this respect, the Framework cannot, thankfully, deliver the outcome envisaged by its original proponents who asserted:

> *"Self-certification means that the question of whether a particular economy implements internationally recognised privacy principles is a question for the competent authority within the economy itself. The Australian view is that there is no need for any externally imposed test of adequacy for member economies"*[54]

We have now hopefully moved beyond this naïve ambition. The APEC Privacy Subgroup has increasingly recognised the need to take account of developments in other international fora, specifically the work of the OECD Working Party on Information Security and Privacy, and to engage with the European Union, as the different approaches must ultimately be reconciled. An initial APEC-EU officials meeting was held in Montreal in September 2007 and there is now a commitment to at least annual meetings and to liaison between these meetings.

## Effect on regional privacy protection

Some of the early fears that the APEC Framework could potentially undermine the effect of domestic privacy laws should by now have been largely dispelled, although it is taking time for this to be realised, particularly in Europe. The existing laws of many APEC members clearly set higher or more specific standards than the APEC privacy principles, and it has now been repeatedly stated in the Subgroup deliberations that there is no intention to detract from the need to comply with the requirements of domestic privacy laws. Subscription to the APEC Framework, as a voluntary non-binding instrument, could not in any case 'trump' domestic legal obligations.

This means in practice that the APEC Framework and its Principles cannot have the effect of *reducing* the existing level of privacy protection either for the citizens of any member economy, or for indviduals in any other country whose personal information is transferred into an APEC economy.

---

53 The Australian Law Reform Commission has just completed a three year review of Australian privacy law (http://www.alrc.gov.au/inquiries/current/privacy/index.htm ). While its final report is not yet public, indications are that it will not recommend any weakening of the trans border transfer principle (NPP9) currently applying to parts of the private sector, and that it will recommend extension of the coverage of the principle to more of the private sector and to government agencies

54 Australian delegation [2003] An APEC Approach to Privacy Protection, Paper 2003/SOM/ECSG/003 for the APEC ACSG meeting, Thailand, February 2003, page 4.

The APEC Cross Border Privacy Rules scheme, as a way of implementing the Framework alongside domestic laws, would appear to offer the advantage of having businesses conduct a level of self-assessment which goes well beyond what is required by most of those privacy laws, which are almost all complaint based, with a default untested assumption that data controllers are complying with the law. From draft assessment criteria under discussion in the Pathfinder project groups, the level of detail provided to 'accountability agents' could also exceed even that required by those European laws which require registration by data controllers. A crucial unanswered question is whether the self assessment details would be made public, or whether a participating business could provide a lesser level of detail in its public privacy notices, statements or policies. The former would be preferable, to contribute to the transparency which is recognised as an essential feature.

Business stakeholders in the Pathfinder projects continually remind other participants that the CBPR mechanisms are not intended to cover compliance with all privacy principles and should focus only on those issues that arise directly from a proposed cross-border transfer. However, it is difficult to see how neat boundaries can be drawn, and it will be very inefficient if a business has to subject itself to multiple overlapping assessments – of compliance with all the requirements of domestic law in the jurisdictions in which it has operations and a separate assessment of its CBPR compliance for exports to other economies.

It will theoretically be possible for businesses to develop a suite of different privacy policies to meet the varying standards required in different APEC economies, with a Cross Border Privacy Rules document as a minimum 'floor' for transfers to economies without substantively higher standards. As I have suggested above, even this would mean a higher level of protection in those countries than would otherwise exist. But it seems unlikely that many businesses would expose themselves to the negative media coverage that such a selective compliance approach would potentially attract. It seems more likely that those businesses that see some value in the CBPR approach will find it in their interests to streamline privacy compliance as much as possible, with one set of notices, statements and policies explaining compliance with *all* relevant requirements, both domestic and international. This would effectively mean a levelling up to a highest common standard.

It remains unclear to most commentators, and to civil society stakeholders, what real benefits the APEC CBPR approach (or for that matter the EU BCR developments) offer businesses, except perhaps a few information intensive multi-nationals who wish to outsource data processing to a range of different countries and can afford to devote substantial resources to writing the documents and getting them assessed. The vast majority of businesses, including most small and medium sized enterprises in all countries, would almost certainly prefer clear legal obligations, enforced only in the event of a breach, and in the knowledge that outsourcing to some destinations was 'off-limits'.

On the other hand, there are some potential collateral benefits from implementation of the APEC Framework through a CBPR approach as a complement to domestic legislation wherever that can be achieved. These benefits include a higher level of self-assessment and independent auditing of privacy compliance than would otherwise occur and faster development of cross border enforcement cooperation mechanisms.

## Conclusion

The APEC Privacy Framework is in my view neither a particularly good alternative model for balancing privacy protection and free flow of information nor a major threat to existing levels of privacy protection.

Differences between the APEC Framework and the other international privacy instruments are not as great as has been suggested, while the deficiencies and obstacles to effective implementation are very similar.

The APEC Framework is no longer capable, if it ever was, of being a 'trojan horse' for self-regulation. It may however provide one route amongst many towards effective privacy protection.