**Annex C**

**to APF Submission to Senate Legal & Constitutional Committee Inquiry into the Privacy Act 1988, March 2005**

# APEC's Privacy Framework: A new low standard

***Professor Graham Greenleaf***

*[Lead article in Privacy Law and Policy Reporter, Vol 11 No 5 ([2005] 11(5) PLPR) – see http://members.iinet.net.au/~greenleaf/plpr/]*

The APEC (Asia-Pacific Economic Cooperation) economies have adopted what is now called the *APEC Privacy Framework*, the most significant international privacy instrument since the EU privacy Directive of the mid-1990s. APEC Ministers at their November 2004 meeting in Santiago, Chile, announced their endorsement of the Framework, which had been developed over the last two years by APEC's Economic Commerce Steering Group (ECSG) Privacy Subgroup.

US Secretary of State Colin Powell, endorsing the Framework, warned APEC ministers that a multiplicity of privacy standards could create confusion in the marketplace and impede information flows that the US considers vital to conducting business globally. Powell endorsed 'region-wide privacy policy compatibility' based on the APEC Framework[1].

The APEC Framework[2] consists of a set of nine 'APEC Privacy Principles' in Part III, 'Implementation' in Part IV, plus a Preamble and Scope note in Parts I and II. However, Part IV is unfinished, as it only includes Section A 'Guidance for Domestic Implementation' but does not yet include Section B on the 'cross-border elements', which it states 'will be addressed in the Future Work of the Privacy Sub Group'. As a result of this omission, the full significance of the APEC Framework cannot yet be assessed because we do not know whether Section B will attempt to restrict data export limitation laws in the Asia-Pacific.

The nine APEC Privacy Principles deal with the topics normally found in international or national sets of privacy principles. APEC considers that the

---

[1] See APEC Press Release for 20 November 2004 at <http://www.apec.org/>

[2] Available at the above address; see also <http://www.bakercyberlawcentre.org/appcc/> for copies of this and previous draft versions, and commentary.

OECD privacy Guidelines of 1980 ‘represent the international consensus’, but only claims that its Framework is 'consistent with the core values’ of the Guidelines. The Framework is in fact weaker in significant respects than the OECD Guidelines, to some extent in its principles but particularly in its implementation requirements. It also shares weaknesses with the twenty year old OECD Guidelines, whereas later instruments such as the EU Directive have strengthened those aspects. These shortcomings are summarised below. Such criticisms were made to APEC’s ECSG during its consultations[3], but the Principles in its final Framework are little different from those in its Consultation Draft of April 2004.

## Implementation and significance

To understand the APEC Framework it is necessary to look at what it does and does not try to do. The Framework is primarily ‘intended to provide clear guidance and direction to businesses’, mentioning business needs frequently in its Preamble. Although its application to government is mentioned rarely in the Preamble, the commentary on Part II states clearly that the Framework applies to both the public and private sectors.

The implementation aspects in Part IV Section A are non-prescriptive in the extreme. They state that members ‘should take all necessary and appropriate steps’ to identify and remove or avoid ‘unnecessary barriers to information flows’ (I). They do not require any particular means of implementation, stating instead that the means of implementing the Framework may differ between countries (‘Member Economies’ in APEC-speak), and may be different for different Principles, but with an overall goal of compatibility between countries. No central enforcement body is required, only some central access point(s) for general information are recommended. (II). They advocate education and publicity to support the Framework (III). They advocate ‘ample’ private sector (including civil society) input into the development and operation of privacy regimes (IV). They state that a country’s privacy protections ‘should include an appropriate array of remedies for privacy protection violations, which could include redress, the ability to stop a violation from continuing, and other remedies’, and these should be ‘commensurate with the extent of the actual or potential harm’. Legislation is not required (V). Countries should also provide to APEC periodic updates on their Individual Action Plan (IAP) on Information Privacy (VI). In essence, Part IV exhorts APEC members to implement the Framework without requiring any particular means of doing so, or any means of assessing whether they have done so.

---

[3] See for example the submission to the ECSG of the Asia-Pacific Privacy Charter Council (APPCC) at <http://www.bakercyberlawcentre.org/appcc/APEC_APPCCsub.htm>

The APEC Framework is therefore considerably weaker than any other international privacy instrument in terms of its implementation requirements. Even the OECD Guidelines required legislative implementation (para 19(a)).

On the other hand, Member Economies are not prevented from adopting privacy rights stronger than the Framework's Principles: they do not require a ceiling on privacy protection.

**The missing 'cross-border elements'**

It is possible that limits on the strength of regional privacy laws may still emerge from the missing Part IV Section B 'cross-border elements'. At this stage the Framework does not require any APEC member to allow data exports to other APEC members who (in some yet-to-be-specified way) implement the Framework. Guarantees of a free flow of personal information to a country as a 'reward' for its observance of minimum levels of privacy protection are an essential feature of all previous privacy instruments (only the EU privacy Directive goes beyond that and requires data export limitations as well). So it would not be surprising *in principle* if the APEC Framework attempted to do this, and this was suggested early in APEC's deliberations. Australia was originally proposing some type of self-certification mechanism for assessing whether Members Economies had implemented the Principles.

The Framework has a bias for free flow of information over privacy protection: its Preamble refers to 'ensuring' free flow of information which is 'essential', but only refers to 'encouraging' privacy protection; it does not include any 'data export limitation' principle, (except the soft US-inspired 'due diligence' requirement of Principle IX); it does not even explicitly recognise that there can be legitimate privacy reasons for restricting data exports (a weakness compared with the OECD Guidelines).

These factors give some reason to be cautious and conclude that we do not know what the Framework means until Part IV Section B is completed. It could still contain 'free flow of information' requirements that have the effect of requiring a weakening of existing and future data export laws in the Asia-Pacific. However, it could also turn out to be as innocuous and non-prescriptive as Section A. The 2005 Work Agenda for the ECSG Privacy Subgroup does not indicate development of any mandatory 'free flow' requirements.

**The APEC Privacy Principles – A low standard**

The scope of the Principles (Part II) is largely uncontentious. Personal information is defined as 'any information about an identified or identifiable individual'. Organisations acting as agents for another are not to be regarded as responsible for compliance, but their principals are. Personal, family and

household affairs are excluded. Publicly available information is excluded from the requirement that individuals consent to its collection.

The wide differences between APEC economies are used to justify Member Economies creating local exceptions to the Principles which are not limited by any list of categories. Instead, the only limits on allowed exceptions are that they should be (a) proportional to their objectives, and '(b) (i) made known to the public; *or*, (ii) in accordance with law' (emphasis added). This last use of 'or' (rather than 'and') appears extraordinarily broad: it allows laws authorising secret *classes* of exceptions (not just secrecy in implementation, as in some forms of surveillance); and it allows exceptions to be created by a business merely by public notice. In both cases the only check on these exceptions are that proportionality is observed.

The nine APEC Privacy Principles (I – IX) are now reviewed briefly[4].

***I Preventing Harm*** – The sentiment that privacy remedies should concentrate on preventing harm is unexceptional but it is bizarre to elevate it to a privacy principle because it neither creates rights in individuals nor imposes obligations on information controllers. To treat it on a par with other Principles makes it easier to justify exempting whole sectors (eg small business in Australia's law) as not sufficiently dangerous, or only providing piecemeal remedies in 'dangerous' sectors (as in the USA). It would make better sense in Part IV on implementation, as a means of rationing remedies, or lowering compliance burdens.

***II Notice*** – APEC says clear statements should be accessible to individuals of the purposes of collection, possible types of disclosures, controller details, and means by which an individual may limit uses, access and correct their information. Reasonable steps should be taken to provide notice before or at the time of collection. APEC does not however require that 'notice' should be by 'notices' given to individuals (it shares this weakness with the OECD Guidelines).

***III Collection limitation*** – APEC shares the weaknesses of the OECD's collection principle in stating only that information collected should be 'relevant' to the purpose of collection, but not that only the minimum information should be collected. While APEC requires that information be collected by 'lawful and fair means', it does not limit collection to lawful purposes.

---

[4] More detailed criticisms may be found in G Greenleaf 'The APEC privacy initiative – 'OECD Lite' for the Asia-Pacific?' in *PL&B International*, Jan/Feb 2004 pgs 16-18

***IV Uses of personal information*** - APEC has adopted the weakest possible test of allowable secondary uses, that it only need be for 'compatible or related purposes', a version of the OECD test of 'not incompatible' purposes. In addition to the usual further exceptions of individual consent and where authorized by law, APEC adds "when necessary to provide a service or product requested by the individual". This could easily be abused if businesses could have the unrestricted right to determine what information available to them was needed for them to decide whether to enter into a transaction, with no need to notify the individual concerned.

***V Choice*** – APEC requires that, where appropriate, individuals should be offered prominent, effectively and affordable mechanisms to exercise choice in relation to collection, use and disclose of their personal information. 'Choice' has been elevated to a separate Principle, an approach not taken elsewhere. Since consent is already an exception the collection and use and disclosure Principles, this Choice Principle only adds an emphasis on the mechanisms of choice. Its wording does not (and should not) imply that consent can override other Principles. It also reiterates that APEC does not require choice in relation to publicly available information, and other exceptions 'where appropriate'.

***VI Integrity of Personal Information*** – APEC requires that personal information should be accurate, complete and kept up-to-date to the extent necessary for its purposes of use. This is uncontentious, except that it (like the OECD), it does not include any deletion requirement.

***VII Security Safeguards*** – APEC requires information controllers (not their agents) to take appropriate safeguards against risks to personal data, and proportional to the likelihood and severity of the risk and the sensitivity of the information.

***VIII Access and Correction*** – APEC's access and correction rights are made more explicit than the OECD's, but are also subject to explicit exceptions where (i) the burden or expense would be disproportionate to the risks to privacy; or (ii) for legal, security, or confidential commercial reasons; or (iii) the privacy of other persons 'would be violated'. These exceptions are very broad and it does not seem that APEC's requirement of proportionality for exemptions applies to them. The dangers of incorrect information are greater where access is prevented by an exception, but APEC has not addressed the question of whether the right of correction depends on their being a right of access.

***IX Accountability*** – APEC's requirement that there be an accountable information controller is uncontentious. It is coupled in IX with a requirement that where information is transferred to a third party (domestically or internationally) this requires either consent or that the discloser exercise due diligence and take reasonable steps to ensure that the recipient protects the

information consistently with the APEC Principles. This is a very soft substitute for a Data Export Limitation principle.

These APEC Privacy Principles do not include the OECD Principles concerning Purpose Specification (only partly implied by the Notice Principle) or Openness (not covered by APEC's Notice Principle or its right of access). Nor do they include any stronger principles contained in any of the region's privacy legislation developed since 1980. They are at best an approximation of what was regarded as acceptable information privacy principles twenty years ago.

**The effect on developing APEC countries**

If the concerns expressed here about the missing Section B prove to be unfounded, then the APEC Framework will not have any explicitly harmful effects on countries that already have privacy laws. If it encourages some of the many regional countries that do not have any privacy laws to adopt laws based on the Framework, it could have beneficial effects, provided it is not regarded as a ceiling on either what is allowable or desirable.

A lot will depend on how the Framework is 'sold' to these developing countries. The US government is I understand allocating USD$100,000 to fund the implementation of the Privacy Framework. through Technical Assistance Seminars on Domestic and International Implementation, to be conducted by a private consultant. If so, then brief given to the consultant, and the extent of supervision by the US government, will be important determining factors. The consultant to 'sell' the Framework is likely to be former Australian Privacy Commissioner Malcolm Crompton.

**The global implications**

A more detailed comparison between the APEC principles and the EU's requirements for findings of 'adequacy' is needed beyond the simple observation that the APEC principles appear weaker than those of the EU, but is beyond the scope of this article. The non-prescriptive approach to implementation and the wide scope for exemptions means that almost everything will depend on national implementations. The relationship between the Framework and the EU privacy Directive also cannot be answered until the missing Part B is completed and the interaction between the two sets of 'cross-border elements' is known. It seems unlikely that adherence to the APEC Framework will *by itself* play a significant role in APEC countries obtaining a finding of 'adequacy' by the EU.

*Graham Greenleaf, University of New South Wales Faculty of Law and General Editor*

*Other articles by Graham Greenleaf about the APEC Framework may be found on his website <http://www2.austlii.edu.au/~graham> and in various issues of PLPR Vol 10.*