The APEC privacy initiative: 'OECD Lite' for the Asia-Pacific?

Graham Greenleaf[*]
27 January 2003

[Shorter version of this paper are published in *Privacy Laws and Business International Newsletter* Issue 71 (UK) and (2004) Vol 10 Issue 10 *Privacy Law & Policy Reporter* (Australia)]

The twenty-one APEC economies (Asia-Pacific Economic Cooperation) commenced development in 2003 of an Asia-Pacific privacy standard, and in 2004 may develop a procedure for handling data export limitation issues[1]. This may become the most significant international privacy initiative since the European Union's privacy Directive of the mid-1990s.

It is a Janus-faced initiative. It has the potential to encourage the development of stronger privacy laws in the those APEC economies that at present provide little privacy protection (the majority), and to help find a regional balance between protection of privacy and the economic benefits of trade involving personal data. It also presents considerable potential dangers to long-term regional privacy protection if it becomes a means by which the APEC economies accept a second-rate standard. Globally, a high APEC standard could be a means of resolving international data export issues, but low APEC standards could entrench a privacy confrontation between Europe and the Asia-Pacific. The history to date of the APEC initiative shows that the dangers are as great as the potential benefits, but a valuable outcome for privacy protection is still possible.

Background and process

At the APEC E-Commerce Steering Group meeting in Thailand in February 2003, Australia put forward a proposal for the development of APEC Privacy Principles using the 20 year old OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980)[2] as a starting point, and implementation mechanisms)[3]. A Privacy Sub Group was set up comprising Australia (chair), Canada, China, Hong Kong, Japan, Korea, Malaysia, New Zealand, Thailand and the United States, under the chairmanship of Mr Peter Ford (Australia). The Privacy Sub Group met again in August (Thailand), and in September (Sydney, Australia). It meets again in February 2004 (Santiago, Chile), when it may finalise the 'APEC Privacy Principles' and move on to implementation measures.

APEC's draft privacy principles are less than a year old, but have already reached their eighth draft. The process has become increasingly secretive. Versions 1-3 were

---

[*] Professor of Law, University of New South Wales; Director, Baker & McKenzie cyberspace Law and Policy Centre <http://www.bakercyberlawcentre.org/>, Chair, drafting committee, Asia-Pacific Privacy Charter Council <http://www.bakercyberlawcentre.org/appcc>

1 For information on APEC and its 21 member economies, see the APEC Secretariat home page <http://www.apecsec.org.sg/>
and<http://www.cba.hawaii.edu/apec/home.htmhttp://www.cba.hawaii.edu/apec/home.htm>

2 OECD, Paris, 1980 <http://www1.oecd.org/publications/e-book/9302011E.PDF>

3 These documents can be obtained at <http://www.apecsec.org.sg/> in the directory Publications / Publications and Library / E-Commerce

made public by the Chair[4], but since version 4 drafts have not been available for general distribution. Consultations are supposed to take place in each participating economy, but the extent to which these are meaningful varies enormously between jurisdictions. For example, in Australia there is no consultation outside government since version 1, but in the USA civil society and business groups are consulted by the US representatives to APEC on each draft. The Sydney meeting involved a public presentation , but with no public disclosure of the current draft, so few attendees were meaningfully informed. Mr Ford has stated that a public draft will be available after the February meeting, but the extent to which any public consultation is proposed after that date is unknown.

Deficiencies of the draft APEC Privacy Principles

To summarise this already lengthy drafting history[5], Version 1 of the APEC Guidelines was already 'OECD Lite'[6] because it did not even include all of the 1980 OECD privacy Guidelines, , and also because those 1980 standards were an inadequate starting point. Version 2 was 'not quite so Lite'[7] including some strengthening of the privacy Principles, and moving in the direction of adopting the rest of the OECD Guidelines concerning implementation. Versions 3-6 revoked the progress of Version 2, weakening the draft even further than Version 1, a process which appeared to coincide with serious United States participation in the process)[8].

The current version (penultimate draft of Version 8[9]), accompanied by an Explanatory Memorandum, is a considerable improvement, and goes some distance toward restoring equivalence with Part II of the OECD Guidelines (OECD's 8 privacy principles (PPs)). However, it still contains four types of serious weaknesses as privacy protection, detailed below, making it of questionable value as an Asia-Pacific standard.

(1) Weaknesses inherent in the OECD Principles

First, the APEC PPs are based on OECD Principles more than twenty years old, the inadequacies of which have been identified by authors over the years[10]. Even the Chair of the Expert Group that drafted them, Justice Michael Kirby, has stressed the need for their revision before they are suitable for the 21st Century[11]. Some of the APEC defects originating in the OECD Principles are:

---

4 See <http://www.bakercyberlawcentre.org/appcc/>

5 For details, see my three articles listed below, based on drafts 1, 2 and 6, available at <http://www2.austlii.edu.au/~graham/>

6 G Greenleaf 'Australia's APEC privacy initiative: The pros and cons of 'OECD Lite'' (2003) 10 (1) PLPR 1

7 G Greenleaf 'APEC Privacy Principles Version 2 - Not quite so Lite, and NZ wants OECD full strength' (2003) 10(3) PLPR 45

8 G Greenleaf 'APEC privacy principles: More Lite with every version' 2003) 10(6) *Privacy Law & Policy Reporter*, LexisNexis Australia

9 The following comments are based on Version 8 (Committee Draft) of 23 January 2004, which is the penultimate draft of Version 8, to be finalised before the Santiago meeting.

10 For example see Roger Clarke 'Beyond the OECD Guidelines: Privacy Protection for the 21st Century' (2000) <http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html>; G Greenleaf 'Stopping surveillance: beyond `efficiency' and the OECD' (1996) 3 PLPR 148

11 Justice Michael Kirby 'Privacy protection, a new beginning: OECD principles 20 years on' <http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html>; (1999) 6 PLPR 25; Justice Michael Kirby '25 years of information privacy law: Where have we come from and where are we going' Privacy Issues Forum, Office of the NZ Privacy Commissioner, March 2003

- The OECD principles only say 'there should be limits on the collection of personal information', failing to define those limits by any objective standard (eg the functions of the collecting organisation[12]). Nor do they include any form of 'purpose justification principle'. APEC PP 3 reflects these weaknesses.
- The OECD test of secondary uses being allowed if they are 'not incompatible' with the purpose of collection is much weaker than common formulations such as 'directly related'. APEC has not yet decided which formulation to adopt, having vacillated between the two (APEC PP 4).
- The OECD has no explicit requirement that notice of purpose of collection must be given *to the individual* at or before the time of collection, although most national legislation in the Asia-Pacific has such a requirement. APEC PP 2, while entitled 'Notice' and specifying that purposes of collection and other matters must be disclosed, still only requires that this be done by 'clear and easily accessible statements' (not notices to be given to individuals). APEC has not yet decided whether to state that notice should be provided 'before or at collection' (wherever practicable). This weakness is reinforced by the Explanatory Memorandum comment that 'one method of compliance … is for personal information controllers to post it on their website'. Such notices are one of the important privacy protections for individuals, and one of the strongest inhibitors on organisations against use for unacceptable purposes.
- The OECD does not include any principles dealing explicitly with identifiers, automated processing, or deletion of data.

(2) Further weakening the OECD Principles

Second, the APEC PPs weaken the OECD Principles in these ways:

- The important OECD Purpose Specification Principle that the purposes of collection 'should be specified not later than at the time of data collection' is not yet included but is under consideration.
- The OECD 'Openness Principle', a broad 'political' limitation which allowed any person to obtain details about the existence and purpose of personal data systems (whether or not they were included in those systems) has been dropped. It is not encompassed by either the APEC Notice principle or the right of individual access.
- OECD PP 4 required all exceptions to the PPs to be 'made known to the public', but APEC replaces this with '(i) made known to the public or (ii) in accordance with law', opening the prospect of a law authorizing the making of secret exemptions to any of the PPs (not just secrecy in the application of an exemption, as may occur in various forms of surveillance).

- Although APEC PP 8's rights of individual access and correction have been made much more explicit (more so that OECD's), there is still under consideration an exemption where 'the information should not be disclosed for legal, security or commercial proprietary reasons'. These blanket exemptions from access are clearly open to abuse, particularly if APEC decides not to require any considerations of proportionality.

---

[12] National legislation often includes this improvement (eg Hong Kong)

- The US is proposing a 'Maximising the Benefits of Privacy Protection' Principle (also not yet agreed), which could elevate 'free flow of information' to a Privacy Principle with the same status as the other Principles, and has been objected to by other all other economies on the grounds that it is only appropriate in the Preamble.

(3) Retrograde new 'Preventing Harm' Principle

APEC PP 1, 'Preventing harm', suggested by the United States, is as follows:

> Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.

While the sentiment behind this may seem unexceptional, it is better to place a 'prevention of harm' principle in the part dealing with implementation and remedies, where it can be used to ration access to remedial processes (as in New Zealand) or to lessen compliance burdens where harm is less likely.

To elevate this to a Principle on a par with the other privacy Principles makes it easier to allow wholesale exemptions from the law like Australia's 'small business' exemption or to argue that there is no need for any uniform privacy laws at all but only for laws in sectors which pose some special danger (as in the USA).

(4) Regional experience ignored as yet

In discussing the APEC process, Hong Kong Privacy Commissioner Raymond Tang has commented[13] that

> While the OECD Guidelines and European Union Directives offered a starting point for discussions my inclination is that a more regiocentric set of guidelines will ultimately emerge in the final drafting.

The most obvious source for such development is the actual standards already implemented in regional privacy laws such as the laws of Korea, Canada, Hong Kong, New Zealand, Taiwan, Australia, and Japan over twenty-five years. Principles stronger than those found in the OECD Guidelines are common in legislation in the region, and many occur in more than one jurisdiction's' laws[14]. However, APEC has as yet not adopted any of these 'regional' improvements.

Some examples of higher standards, in the sense that they are found in at least two regional privacy laws, are as follows:

- Collection objectively limited to where necessary for functions or activities of organisations (HK, Australian Federal, NZ ; Canadian Federal is even stricter);
- Notices upon collection (Australia Federal, NZ, HK, Korea);
- Secondary use only for a directly related purpose (HK, NZ, Australia Federal; Korea is even stricter);

---

[13] Raymond Tang 'Personal Data Privacy: The Asian Agenda' *25th International Conference of Data Protection and Privacy Commissioners*, Sydney, September 2003

[14] For examples, see G Greenleaf 'APEC privacy principles: More Lite with every version' 2003) 10(6) *Privacy Law & Policy Reporter*, LexisNexis Australia

- Right to have recipients of corrected information informed (NSW, NZ);• Deletion after use (HK, NZ, NSW, Korea)

A few improvements

The APEC PPs (Privacy Principles) do include some potential improvements on the OECD principles, all of which are still under consideration:

- A requirement that any exceptions should be 'limited and proportional to meeting the objectives to which the exceptions relate'.
- The limiting of secondary uses to those 'directly related' (discussed above).

A 'limited retention principle', initially supported by New Zealand, Hong Kong, China and Taiwan, has now been removed by consensus from consideration.

implementation measures still undecided

Major parts of the OECD Guidelines as yet not included

APEC draft Version 8 Part IV 'Implementation Mechanisms' simply says 'to be discussed early 2004. Previous versions said that Parts 1,2,4 and 5 of the OECD Guidelines are to be consideredas well as parts of the Asia-Pacific Telecommunity (APT) draft Guidelines. Important OECD provisions not yet in the APEC principles include:

- That they are only minimum standards that may be supplemented (OECD 6).
- A requirement for protection by legislation (OECD 19(a));
- Requirements for 'reasonable means for individuals to exercise their rights' (19(c)), for 'adequate sanctions and remedies' (including against data export breaches) (19(d)), and for 'no unfair discrimination' (19(e)).
- Recognition of the need for greater protection of sensitive classes of data (OECD 3(a));

APEC proposals for self-assessment and data export limits

OECD guideline 17 explicitly sets out three situations when data export restrictions are acceptable (though, unlike the EU privacy Directive, it does not mandate them):

- where the importing country does not 'substantially observe' the OECD Guidelines,
- where re-export would circumvent domestic laws (in effect, where the receiving country does not have its own data export prohibitions); and
- to protect sensitive data not similarly protected overseas.

The OECD guidelines, unlike the EU privacy Directive, do not have any provisions for external assessments of the conformity to the guidelines of the privacy laws of member countries, or of third countries.

APEC's principles do not yet include provisions concerning data exports, or procedures for assessment of compliance with the principles.

The USA is proposing an addition to APEC PP 9, resisted as yet by other participants, that says:

> When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should exercise due diligence and take reasonable steps to ensure the recipient person or organization will protect the information consistently with these Principles.

In Version 6 the Chair suggested a data export limitation Principle based on the approach of allowing transfers only if the *recipient* organisation has taken such reasonable steps. Whether APEC will have a data export principle remains uncertain.

To accompany Version 1 of the *APEC Privacy Principles* Australia suggested[15] five options for compliance assessment which only involve (at their highest) self-certification by governments ('economies' in APEC-speak) concerning their implementation of the *APEC Privacy Principles*. Such self-certification, without any independent verification, is unlikely to engender confidence by overseas trading partners or potential investors, other governments, or on-line consumers. Nor is it likely to satisfy the current requirements of the laws of countries which do include data export limitations (whether within APEC or in other regions). Australia has a clear policy of opposing any 'European-style' external assessments of adequacy of privacy laws[16], and is attempting to advance that policy at a regional level through APEC.

In response, New Zealand Assistant Privacy Commissioner, Blair Stewart, submitted an Option 6[17] which involved a two-tier approach of APEC regional certification. Assessment would involve publicly available recommendations by a 'committee of independent experts', then the 'decision to certify substantial compliance would be by a committee of officials from APEC members'. This independent certification of 'substantial compliance' (the OECD terminiology) would then be recognised by APEC member economies. It is not a radical proposal, but is far in advance of any of the five Australian options in its respect for privacy protection[18].

Global implications

If it was possible to achieve cross-recognition of 'adequacy' between APEC standards and European or other regional standards, this would obviously solve many of the problems of international flows of personal data.

This is unlikely to be achieved by APEC if its privacy principles remain 'OECD Lite', but the draft Version 8 standards show that it is possible that APEC could adopt principles which would only need modest improvements to be acceptable to the EU. Equally important is how APEC resolves the question of a data export principle, and

---

[15] *Privacy Implementation Mechanisms (Version 1)* - see <http://www.BakerCyberlawCentre.org/appcc/oecd_redraft.htm#implementation>

[16] See Attorney-General D William 'Opening Address – APEC Privacy Workshop', Sydney, 13 September 2003, available at <13 September 2003>; for details, see John McGinness, Federal Attorney General's Department Australia 'What's Up In The Asia Pacific ? APEC Privacy Initiatives', *Privacy Issues Forum*, Wellington NZ, 28 March 2003available at <www.privacy.org.nz/media/McGinness.pdf >

[17] Blair Stewart, Assistant Privacy Commissioner, NZ 'A suggested scheme to certify substantial observance of APEC Guidelines on Data Privacy' (APEC E-commerce Steering Group meeting, 2003)

[18] For further discussion, see G Greenleaf 'Australia's APEC privacy initiative: The pros and cons of 'OECD Lite'' (2003) 10 (1) PLPR 1

the related issue of assessments of compliance with the guidelines. After the APEC meeting in Santiago in late February 2004, the approach it is taking should be more clear.