Five years of the APEC Privacy Framework: Failure or promise?

Graham Greenleaf, University of New South Wales[*]
<g.greenleaf@unsw.edu.au>

Abstract: *The APEC Privacy Framework was developed from 2003, adopted by APEC in 2004 and finalised in 2005. It was intended as a means of improving the standard of information privacy protection throughout the APEC countries of the Asia-Pacific , and of increasing the trans-border flow of personal information between those countries. In 2007 a number of 'Pathfinder' projects for cross-border data transfers were launched under the Framework. In the five years since the process commenced, what has it achieved, and what is it likely to achieve? This paper argues that the APEC Privacy Framework has had many flaws from its inception: its Privacy Principles set the lowest standards of any international privacy agreement; and it has no meaningful enforcement requirements. Since then, no attempt has been made to encourage its use as a minimal standard for privacy legislation in developing countries (which might have been useful); the 'Pathfinder' projects leave many questions about what standards they aim to implement; and consumer input into its processes have been largely absent but business influences omnipresent. Despite these flaws, it could still play a usefulr role in the gradual development of higher privacy standards in Asia, provided its priorities are re-oriented. The major developments in Asian privacy protection will come from elsewhere. The paper concludes with suggestions for other directions.*

[*] Earlier versions of parts of this paper have been published before, as the APEC Privacy Framework has developed since 2003 (see Greenleaf 2003a-2008 in references). This paper reconsiders and updates those arguments over five years.

The APEC Privacy Framework

In November 2004 Ministers of the APEC (Asia-Pacific Economic Cooperation) economies, meeting in Santiago, Chile, adopted the *APEC Privacy Framework*, which had been developed during 2003-04 by APEC's Economic Commerce Steering Group (ECSG) Privacy Subgroup. The significance of the 21 APEC economies[1] adopting common information privacy standards cannot be doubted. The APEC economies are located on four continents, account for more than a third of the world's population, half its GDP, and almost half of world trade. The APEC Framework could have become the most significant international privacy instrument since the EU privacy Directive of the mid-1990s (EU, 1995). This is unlikely to be the case, though it may well have some positive effects. However, compared with its potential, the reality seems more like a missed opportunity.

The APEC Privacy Framework (APEC, 2004) originally consisted of a set of nine 'APEC Privacy Principles' in Part III, plus a Preamble and Scope note in Parts I and II. Part IV 'Implementation' included Section A 'Guidance for Domestic Implementation' but did not include Section B on the 'cross-border elements' (including data exports) until it was added in September 2005 Part IV(B) and the Framework completed (APEC, 2005). A Commentary is included.

A brief critique of both the principles and the implementation mechanisms follows. In summary, the Principles in APEC's Privacy Framework are at best an approximation of what was regarded as acceptable information privacy principles twenty years ago when the OECD Guidelines were developed. In relation to implementation, 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. The Framework is therefore considerably weaker than any other international privacy instrument in terms of its implementation requirements. In so far as data exports are concerned, the Framework neither requires, limits nor forbids data export limitations.

A floor or a ceiling? - the status of APEC 'agreements'

Unlike the OECD Guidelines which explicitly state that they are only minimum standards for privacy protection that may be supplemented in national laws by other principles (OECD 1981: 6), the APEC Framework does not at any point explicitly state that there may or may not be national strengthening of its Principles. However, it is hard to see how the Framework could attempt to impose such a ceiling, since almost every privacy law enacted in the region is stronger than the APEC Privacy Principles in various ways (as discussed later, and see Greenleaf, 2005c, 2007 for details). It seems, therefore, that the APEC Framework should be interpreted as recommending a minimum desirable standard for privacy protection (with exceptions), but not a maximum standard: a floor but not a ceiling for privacy protection (see Greenleaf 2005d for details). Furthermore, since APEC is a political grouping which does not have a constitution[2], operates by consensus, and undertakes commitments on a voluntary

---

[1] See Member Economies list at <http://www.apec.org/apec/member_economies.html>

[2] "APEC is the only inter governmental grouping in the world operating on the basis of non-binding commitments, open dialogue and equal respect for the views of all participants. Unlike the WTO or other multilateral trade bodies, APEC has no treaty obligations required of its participants. Decisions made within APEC are reached by consensus and commitments are undertaken on a voluntary basis." – 'About APEC' from APEC secretariat website at <http://www.apecsec.org.sg/apec/about_apec.html>

basis, APEC 'agreements' such the Framework do not have any legal status, and are best seen as agreed aspirations. Nevertheless, their practical effect is often very significant.

APEC Privacy Principles – A brief critique

The nine APEC Privacy Principles deal with most of the broad topics normally found in international or national sets of privacy principles: collection, quality, security, use, access to, and correction of personal information.

Definitions and exemptions (Part II)

Before considering the Part III Principles, the Part II definitions need brief mention though they are are largely uncontentious. '*Personal information*' is defined as 'any information about an identified or identifiable individual'. The commentary clarifies only that the information may be 'put together with other information' to identify an individual and that legal persons are not included. '*Personal information controller*' is defined as meaning 'a person or organization who controls the collection, holding, processing or use of personal information', so there can be multiple controllers. However, organisations acting as agents for another are not to be regarded as responsible for 'ensuring compliance', but their principals are. Agents appear to be exempt from any direct responsibility to the data subject for breaches of the Principles (a) by actions contrary to their principal's instructions; and (b) even if they are aware they are in breach.

'*Publicly available information*' is given a broad definition, including the flexible category of information 'that the individual knowingly makes or permits to be made available to the public'. However, such information is only excluded from the requirement that individuals be given notice of its collection by third parties collecting it. The APEC Principles do not give the collector of publicly available information any right, per se, to disclose the information to others. They can, however, use it for the purpose for which they collect it. They must also take reasonable steps to keep it secure, as it is still personal information. *Personal, family and household affairs* are excluded, but there is no further list of exemptions for the press, national security, emergencies etc.

The wide differences between APEC economies are used to justify Member Economies creating local exceptions to the Principles unconstrained by any APEC list of categories of allowable exceptions. 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,* (b)(ii) in accordance with law' (emphasis added). This last use of 'or' appears to be a drafting error and should say 'and', otherwise it would mean any organisation could create exceptions merely by announcing them (see Greenleaf, 2005a, for details). For comparison, OECD principle 4 states that exceptions should be as few as possible, and made public. It is not clear whether these limits on exceptions (weak though they are) also apply to those exceptions already included in the Principles (eg to Principle VIII Access and Correction). They should apply, and it is a weakness that this is not clear.

The nine Principles – strengths and weaknesses

Each APEC Principle I-IX is now summarised, and main weaknesses or strengths noted, but without detailed comparison to other laws in the region (for which see Greenleaf 2005c, 2007).

I Preventing Harm

The sentiment that privacy remedies should concentrate on preventing harm ('should be designed to prevent the misuse of such information' and should be 'proportionate to the likelihood and severity of the harm threatened') is unexceptional but it is strange 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 as not sufficiently dangerous (eg small business in Australia's law, or in the 2005 Chinese 'Expert Draft' proposals: see Greenleaf, 2008a), or only providing piecemeal remedies in 'dangerous' sectors (as in the USA). It is not clear from APEC's Principles whether 'harm' covers distress, humiliation etc. It is also arguable that there should be a right to privacy in some situations independent of any proven harm, such as where there is the intentional large-scale public disclosure of private facts. This 'principle' 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, disclosing the purposes of collection, possible types of disclosures, controller details, and means by which an individual may limit uses, and 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 some explicit form of notice (electronic or paper) given to individuals (and nor do most existing laws in the region). It can be argued that in many cases this will be the only form that reasonable steps can take. APEC is not explicit that notice of collection must be given to a data subject where their personal information is collected by a third party but the Commentary clearly implies that it should. APEC's Principles are stronger than the OECD's on this point.

III Collection limitation

APEC requires only that information collected should be limited to what is 'relevant' to the purpose of collection, but not that only the minimum information should be collected. It shares the weaknesses of the OECD's collection principle which only say 'there should be limits on the collection of personal information'. Existing laws in the region are usually more strict, with collection objectively limited to where necessary for the functions or activities of organisations. While APEC requires that information be collected by 'lawful and fair means', it does not limit collection to lawful purposes, in contrast with existing laws in the region.

IV Uses of personal information

APEC has adopted the weakest possible test of allowable secondary uses, that they only need be for 'compatible or related purposes' (a version of the OECD test of 'not incompatible' purposes). Most existing laws in the region are stricter than this, requiring that secondary uses be 'directly related' or within the 'reasonable expectations' of the data subject. In addition to the usual further exceptions of individual consent and 'where authorized by law', APEC adds another exception '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, effective and affordable mechanisms to exercise choice in relation to collection, use and disclosure of their personal information. Since consent is already an exception to the collection and use and

disclosure Principles, this Choice Principle only adds an emphasis on the mechanisms of choice, and could be seen as redundant. It is not in other sets of Principles. The elevation of choice to a separate principle poses some risk of interpretations that would support bundled consent. However, the wording of the Choice Principle does not (and should not) imply that consent can override other Principles, so it does not imply that individuals should be able to 'contract out' of the security, integrity, access or correction Principles.

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 (like the OECD), it does not include any deletion requirement.

VII Security Safeguards
APEC requires information controllers (but not their agents) to take appropriate safeguards against risks to personal data, proportional to the likelihood and severity of the risk and the sensitivity of the information. This is uncontentious, except it is hard to see why agents should not also be liable.

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. However, APEC says individuals should have the right to challenge refusals of access. 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 there being a right of access. Nor have most existing laws.

IX(a) Accountability
APEC's requirement that there be an accountable information controller is uncontentious, but is limited by the exclusion of agents from liability (discussed earlier).

IX (b) Due diligence in transfers
Accountability is coupled in principle IX with a requirement that where information is transferred to a third party (domestically or internationally) this requires either the consent of the data subject 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 sub-principle was proposed by the USA. This is a soft substitute for a Data Export Limitation principle, and may leave the data subject without a remedy against any party where the exporter has exercised due diligence but the importer has nevertheless breached an IPP. There is no remedy against the exporter, and none against the importer if it is in a jurisdiction without applicable privacy laws, unless there is a contractual clause requiring APEC compliance in a jurisdiction where consumers can enforce such clauses benefiting third parties (ie where doctrines of privity of contract do not prevent this).

Five bases for criticism

There are five distinct forms of criticism that may be leveled at the APEC Privacy Principles (see Greenleaf, 2005a for more detail), and which are inherent in my above summary.

(1) ***Weaknesses inherent in the OECD Principles*** First, the APEC Privacy Principles are based on OECD Principles more than twenty years old, and only improve on them in minor respects. The inadequacies of the OECD Principles have been identified by authors over the years (eg Clarke, 2000 and Greenleaf, 1996). 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 Kirby, 1999).

(2) ***Further weakening of the OECD Principles*** 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. APEC states that the OECD privacy Guidelines 'represent the international consensus', but only claims that its Framework is 'consistent with the core values' of the Guidelines (APEC, 2005, Preamble, para 5), not that they reflect them on all points. The APEC Privacy Principles improve on some OECD Privacy Principles in minor ways, and they are weaker than others in some ways. They do not include the OECD Privacy Principles concerning Purpose Specification or Openness, and are therefore weaker on those counts.

(3) ***Potentially retrograde new Principles*** The only new principles, 'Preventing harm' and 'Choice', while capable of benign interpretations, carry inherent dangers and have little to recommend them.

(4) ***EU compatibility ignored*** While some countries in the region have difficulties in accepting that the EU should judge the 'adequacy' of their privacy laws, ignoring the EU standard is not necessarily an approach that other APEC countries would prefer. The principles in the EU Directive are also the most widely implemented privacy principles, and for that reason deserve comparison as a standard. New principles found in the EU privacy Directive (EU, 1995), such as its automated processing principle, do not seem to have received any consideration by APEC, and the question of EU consistency does not seem to have been explicitly addressed in their considerations. This might be considered a missed opportunity.

(5) ***Regional experience ignored*** The most obvious source that an Asia-Pacific regional instrument could be expected to draw from 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. These include principles concerning collection directly from the individual, data retention, notice of corrections to third party recipients, data export limitations, anonymity, identifiers, sensitive information, and public registers (for details see Greenleaf, 2005c and Greenleaf, 2007). APEC has not adopted any of these 'regional' improvements. Without suggesting that APEC should have embraced all of them, the Framework's failure to include any other new principles means that it ignores or rejects the experience of those Asia-Pacific countries that do have privacy laws and have consistently included Privacy Principles which go beyond those of the OECD, and very often share these new Privacy Principles across multiple Asia-Pacific jurisdictions. The APEC Principles therefore do not represent any objective 'consensus' of existing regional privacy laws, unless it that of the lowest common denominator of every IPP in the region.

What have the Principles achieved after five years?

The APEC Privacy Principles are of no domestic significance to the economies in the Asia-Pacific region that already have general information privacy laws (Australia, Canada, New

Zealand, Hong Kong SAR, Japan and South Korea – Taiwan is debatable), because the Principles in all of those laws exceed the level of protection provided by the APEC Principles at various points. There may be a few minor points where specific APEC principles such as the Security Principle may have better drafting than local laws, but in general these jurisdictions have 'nothing to learn' from APEC. In Australia's current review of its privacy laws, the APEC principles are being largely ignored.

Since 2003 when the first APEC drafts appeared, there has not been a single new APEC jurisdiction (or other Asia-Pacific country for that matter) that has introduced an information privacy law, or any other known method of implementing privacy principles. The 2005 'Expert Draft' proposed law in China (Greenleaf, 2008a, 2008b) was roughly congruent with the APEC Principles (though there is no evidence it was influenced by it), but now seems unlikely to proceed. As a means of encouraging the better protection of privacy protection across APEC to a minimum agreed standard, the APEC Privacy Framework seems to have been a conspicuous failure so far.

Implementation – Exhortations only

The Framework's implementation aspects in Part IV Section A ('Guidance for domestic implementation'), provisions I – VI, 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), but do not include any similarly strong injunctions to take 'all necessary and appropriate steps' to protect privacy. The bias is clear.

The Framework does not require any particular means of implementation of the Privacy Principles, 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. (II).

In (II) it is made clear that anything ranging from complete self-regulation unsupported by legislation, through to legislation-based national privacy agencies is acceptable to APEC:

> 'There are several options for giving effect to the Framework and securing privacy protections for individuals including legislative, administrative, industry self regulatory or a combination of these methods under which rights can be exercised under the Framework.'
>
> 'In practice, the Framework is meant to be implemented in a flexible manner that can accommodate various methods of implementation, including through central authorities, multi-agency enforcement bodies, a network of designated industry bodies, or a combination of the above, as Member Economies deem appropriate.'

There is mention of the value of complainants having a choice of remedies 'commensurate with the extent of the actual or potential harm to individuals resulting from such violations' (V).

Legislation is mentioned as one means of providing remedies but is not required or even recommended (V). In contrast, even the OECD Guidelines 'Part 4 National Implementation' state that 'Member countries should in particular endeavour to (a) adopt appropriate domestic legislation' (OECD 19(a)) and a range of other means including 'reasonable means for individuals to exercise their rights' (19(c)), 'adequate sanctions and remedies' (including against data export breaches) (19(d)), and for 'no unfair discrimination' (19(e)). The OECD support for legislation is tepid, but APEC's is non-existent.

What verifiable implementation is there after five years?

What criteria are to be used to measure whether a chosen implementation measure is sufficient to implement the APEC Privacy Principles? APEC only states 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'. No external means of assessment are suggested. This now creates problems for the 'Pathfinder' projects, as discussed below.

Nor does APEC require that there by any central enforcement body (no matter what enforcement approach is adopted), but merely recommends some central access point(s) for general information. (II). 'Pathfinder' project 5 is now supposed to document this.

Member economies are also supposed to provide to APEC periodic updates on their Individual Action Plan (IAP) on Information Privacy (VI). There are no provisions for any third party assessments of these IAPs in terms of their compliance with the Framework. Development of this IAP content was supposed to have started after the second Implementation Seminar in 2005, but as yet there is no privacy-related content in the IAPs on the APEC ESCG website (2007), so that aspect of external validation of compliance has also failed.

APEC advocates education and publicity to support the Framework (III). It advocates 'ample' private sector (including civil society) input into the development and operation of privacy regimes (IV), but as we will see, this has so far resulted in the inclusion of business interests but exclusion of consumers.

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. No means of assessment have yet been developed. The APEC Framework is therefore considerably weaker than any other international privacy instrument in terms of its implementation requirements, and its practices.

Data export issues

A key purpose of the APEC Privacy Framework is to increase the free flow of personal information between APEC economies. We first need to see how other international privacy agreements address this issue.

OECD and EU approaches – allowing and requiring

The OECD Guidelines require that member countries do not impede the free flow of personal information to other OECD countries that do 'substantially observe' the Guidelines. They also explicitly set out three situations when data export restrictions are acceptable: 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 (OECD, 1981: 'Part 3 - Basic Principles of International Application', guideline 17).

The novel development in the EU Directive was that, while it required that there be free flow of personal information to other EU countries (on the basis that they were all required to implement the standards of the Directive in their national laws), it also required member countries to prohibit personal data exports to non-EU countries unless the standards required

by the EU for personal data exports were met (the best known of which is the 'adequacy' standard under A25 of the Directive). In some cases, where the EU's standards were met by a non-EU country, the EU country concerned was not permitted to forbid the export to the non-EU country, thereby guaranteeing a certain degree of free flow of personal information even outside the EU. There is now an Optional Protocol (CoE, 2001) to the Council of Europe privacy Convention 108 (COE, 1981) to the same effect.

There is therefore nothing unusual in an international privacy agreement including a guarantee of free flow of personal information as an inducement to meet an agreed minimum standard of privacy protection. Equally, there is nothing unusual in international agreements recognising that it can be justified to prohibit data exports in some circumstances (OECD Guidelines), and even making such restrictions mandatory (EU Directive).

The APEC Framework's approach – neutrality?

What approach is APEC taking to these issues? It is necessary to look at both the final Framework, and its implementation through the post-2007 'Pathfinder' projects.

When the Framework was released in 2004, it seemed possible that it might seek via the missing Part IV (B) to discourage or prevent data export limitations in regional privacy laws, or attempt to provide guarantees of free flow of personal data within APEC despite such existing export limitations (in force only in Australia, Taiwan, and Quebec). A number of factors supported such an expectation (see Greenleaf, 2007 for a summary), including that embodying such a 'trade-off' in the Framework was suggested by then APEC Privacy Subgroup Chair in his *Privacy Implementation Mechanisms (Version 1)* accompanying version 1 of the APEC principles (APEC drafts, 2003-04; and see Ford, 2003 and Greenleaf, 2003a).

However, such expectations were not been borne out by the September 2005 final version of Part (IV) B. It says nothing directly about personal data exports – either in terms of limitation rules or requirements to allow them. Part IV (B) III 'Cooperative Development of Cross-border privacy rules' only deals with 'recognition or acceptance of organizations' cross-border privacy rules across the APEC region' (APEC Framework Part B, 2005). The final version does not seem to take as strong a position as suggested by the *Consultant's Issues Paper* (Crompton and Ford, July 2005) which proposed that one of three 'implementation objectives' APEC 'should work toward' is that 'prevention of data flow across borders should not be put forward as a generally suitable remedy for privacy infringements that involve two or more economies.' Such discouragement of data export restrictions is not explicitly found in the APEC Framework, and nor is it found in the official Report on the second seminar (APEC ECSG Privacy 2005).

In other words, the final APEC Framework does *not* do any of the following:

(i) Forbid (or even discourage) data exports to countries without APEC-compliant laws (contrast the EU Directive);

(ii) Explicitly allow restrictions on data exports to countries without APEC-compliant laws (contrast the OECD Guidelines and the Council of Europe Convention);

(iii) Require data exports to be allowed to APEC economies that have APEC-compliant laws (or equivalent protections) (contrast any other international privacy agreement).

The Framework's Commentary encourages (iii), but does not discourage (ii). The APEC Privacy Framework is therefore extremely non-prescriptive in relation to data exports, consistent with its general non-prescriptive nature. This means that the fears expressed by some commentators (Greenleaf, 2005c, 2005d) that the APEC Framework might create a data protection 'bloc' which is antagonistic to the EU's 'adequacy' requirements have not been borne out.

Cross-Border Privacy Rules (CBPR) and the 'Pathfinders'

In September 2007 the relevant APEC Ministers endorsed the 'Data Privacy Pathfinder' proposal developed by the Data Privacy Subgroup. Such projects must have the support of a majority of APEC economies, and no veto. The Pathfinder project has 'the goal of developing and implementing an accountable Cross-Border Privacy Rules (CBPR) system within APEC', so as 'to protect the personal information of an individual no matter where in the APEC region that personal information is transferred or accessed'. The Pathfinder proposal is described in its Executive Summary as:

> Thirteen APEC member economies have agreed to develop a framework for accountable flows of personal data across the region, focussing on the use of cross-border privacy rules by business. This will promote consumer trust and business confidence in cross-border data flows. It will support business needs, reduce compliance costs, provide consumers with effective remedies, allow regulators to operate efficiently, and minimise regulatory burdens.

These proposals are not limited to intra-company transfers: they may deal with data exports to any other company in any other (APEC) economy.

The Project Work Plan says 'An economy's expression of support indicates support for an overarching approach for developing and implementing a CBPR system. Economies may then consider whether they are able to support and participate in the development and implementation of specific projects.' With Ministerial adoption, all economies now support the Pathfinder process, but are not necessarily involved in projects.

The Pathfinder participants

Of APEC's 21 member 'economies', 13 expressed interest in participating in one or more of the nine Pathfinder projects detailed below, by the time of the September 2007 Ministerial endorsement: Australia, Canada, Hong Kong, Japan, Republic of Korea, Mexico; New Zealand, Peru, Singapore, Thailand, Chinese Taipei (Taiwan), the United States, and Vietnam. By then the International Chamber of Commerce (ICC) had already indicated its interest in participating in all nine projects, as had the USA. The International Chamber of Commerce (ICC) is to lead Pathfinder project 1, Mexico projects 2 and 3, Australia 5, 6 and 7, the USA project 9, and leaders for the others are undecided .

The eight who have apparently chosen not to participate in any of the 'Pathfinder' projects include the People's Republic of China, Indonesia, Malaysia, the Philippines, Papua New Guinea, Russia, and Brunei. China is the most important absentee, as it has been for much of the Data Privacy Subgroup's work.

The Pathfinder projects

There are nine Pathfinder projects that economies can decide to join:

1. CBPR self-assessment guidance for organisations

2. Guidelines for trustmarks participating in a CBPR system ('Develop guidelines for what a trustmark must do in order to be recognised as an APEC CBPR accreditation provider.')

3. Compliance review of an organisation's CBPRs ('Develop guidelines for trustmarks to use when assessing an organisation's compliance with the APEC Privacy Principles.')

4. Directory of compliant organisations ('Develop a publicly accessible directory of organisations that have CBPRs that have been accredited as complying with the APEC Privacy Principles.')

5. Data Protection Authority and Privacy Contact Officer Directory

6. Template Enforcement Cooperation Arrangements

7. Template cross-border complaint handling form

8. Guidelines and procedures for responsive regulation in a CBPR system ('Develop guidelines and procedures (e.g. flowchart) to assist in determining at which stage of the CBPR responsive regulation pyramid a cross-border privacy complaint should be handled and identify the triggers for escalating a complaint to a higher level of the pyramid')

9. Cross-Border Privacy Rules International Implementation Pilot Project (including participating economies identifying businesses willing to participate)

Following clarifications given at the Privacy Subgroup meeting in Lima, Peru, in February 2008, Waters (2008) summarises how the CBPR approach set out in the Pathfinders is supposed to work, 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). In the Pathfinder this is known as 'self-assessment' (project 1). This self-assessment will be based on a standard set of questions, currently being drafted by TRUSTe with input from all participants.

- The document would be assessed by an 'accountability agent' which might be a regulatory agency or a 'trustmark' organisation. Private accountability agents (e.g., trustmarks) would be approved based on a separate trustmark assessment process, guidelines for which are project 2. TRUSTe has also provided a first draft of this document for review by participants.

- Project 3 involves developing guidelines for trustmarks to use when assessing the compliance of organisations with the relevant legal/self-regulatory criteria.

- If assessed as meeting the requirements, the business would be included in a publicly accessible directory of compliant organisations (project 4).

- Regulators will establish mechanisms for cooperation on complaints that involve multiple jurisdictions (projects 5-7).

- 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. A number of US corporations, and TRUSTe have already volunteered, but the Subgroup is seeking a wider group for project 9. This is important given the current preference of Mexico, Japan, Vietnam and a number of other Asian member economies for a trustmark-based approach.'

Unanswered questions about standards

Projects 5-8 aim to increase cooperation between all types of data protection authorities, are not related specifically to CBPR schemes, and are uncontroversial. Project 9 involves making elements of the other projects work together. It is Projects 1-4 that raise questions which are not answered by any of the official APEC Pathfinder documents (Greenleaf, 2008).

Against what criteria does an organisation assess whether its CBPR procedures are good enough (Project 1)?

Similarly, what is the standard of privacy protection to which a trustmark provider must accredit organisations (Projects 2 and 3)? As Waters (2008) puts it:

> 'Another 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 trustmarks, but who will make the decision that a trustmark scheme (or a regulatory agency) meets these criteria? As with organisational assessments, we [civil society organisations] will argue for full transparency with respect to trustmark assessments.'

The APEC Privacy Framework does not provide answers to these two questions, as it is quite open as to what standards different economies may require in order to allow cross-border transfers (see Greenleaf, 2005). The APEC Pathfinder documents are unclear as to where they locate the standards against which particular organisation's cross-border privacy rules are to be measured. Where countries have information privacy laws, there may be limits as to what cross-border transfers can be allowed. But where no laws apply are the standards for cross-border transfers those that consumers would set, or governments – or businesses?

Perhaps the operating assumption here is that (except where a law forbids) any data export is allowable provided the exporter can claim to be adhering to the APEC Privacy Framework. In particular, APEC Principle 10 says any data exporter must either obtain consent or 'exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles'. Is it being assumed that this is enough, and 'accreditation' should be provided on this basis (at least where local laws does not forbid this)? Such an approach may be feasible in relation to the Principles themselves, but the APEC Framework does not state how the sufficiency of any compliance measures are to be assessed, so there is no objective standard of whether the information is 'protected'. At the least, APEC needs to better communicate its intentions and its operating assumptions.

According to Waters, accreditation by a trustmark provider is not the only way to be included in a directory (Project 4), because an 'accountability agent' can also be a 'regulatory agency'. Under what powers regulatory agencies can carry out the assessments required by Projects 2 and 3 remains to be seen.

Waters considers that collective 'adequacy' assessments will eventually be necessary (Waters, 2008), an argument first raised by NZ Assistant Commissioner Stewart in 2003 (see Greenleaf, 2003a):

> '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 Articles 29 and 31 Committee processes. No economy, and in particular no regulator in those economies with a legislated cross border transfer principle … will 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. There is reluctance on the part of some participants to acknowledge this fact; indeed some participants seem to view the Pathfinder project as a replacement for traditional "adequacy" determinations, via a sort of "safe harbour" approach, although it is not clear how this can be reconciled with their acceptance of domestic legislative requirements.'

Potential advantages

An optimistic approach is to hope that this CBPR work will encourage economies with no current privacy legislation to adopt legislation embodying the APEC Principles, on the basis that this will then make it easier for them to utlise the CBPR procedures to secure information flows to their economy.

Waters (2008) also sees some advantages in the 'self assessment' aspects:

> 'The scheme would appear to offer the advantage of having businesses conduct a level of self-assessment which goes well beyond what is required by most domestic privacy laws, which are almost all complaint-based and have a default untested assumption that data controllers are complying with the law. From draft assessment criteria presented in the Lima workshop, the level of detail provided to 'accountability agents' would 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. Civil society organisations will argue for the former.'

'All Present Except Consumers' (A.P.E.C.)?

What role do consumer interests have in APEC's privacy processes? In the development of the Framework, consumers were not invited to participate. The one detailed and critical submission by a consumer organisation (see APEC darfts, 2003-04: APPCC Submission), had no effect. Has anything improved?

The Pathfinder proposal approved by Ministers in 2007 says that one of its 'main objectives' will be 'promoting the development of consultative processes … including … consumer representatives both in the creation of the rules and processes and in their operational review and optimisation.' (APEC, 2007). These objectives are repeated at the outset of the Project Work Plan. However, the nine projects were designed without any input from consumer representatives, in contrast to extensive input from business organisations.

At the time these objectives were under consideration, Privacy International (PI) applied for accreditation to the APEC Data Privacy Subgroup, in the same way that the International Chamber of Commerce (ICC) and another business group (Global Business Dialogue on e-Commerce (GBDe)) are accredited to be represented, with speaking and participation rights. PI's application was declined by the APEC Secretariat in June 2007, with the comment that consumer representatives could ask to join delegations from economies (ignoring the fact that this does not give a right to speak at Subgroup meetings without consent of delegation chairs, or to participate in Pathfinder projects). Both PI and the USA's Electronic Privacy Information Centre (EPIC) made a further application at APEC's Peru meeting in February 2008 for guest membership status. Although there was no apparent objection to this at the Privacy Subgroup meeting, neither application was approved by the ECSG, apparently because one economy objected (APEC works by consensus). The applications are deferred to the next ECSG meeting pending both organisations providing further background information (Waters, 2008).

Consumer groups in various APEC countries have been undecided whether to engage with the APEC processes, or to oppose them. As Canada's Lawson (2007) says 'the process looks very much like a cleverly disguised attempt to establish a low international standard through the back door'. Australia's Waters (2007), commenting on the October 2007 meeting in Montreal between representatives of the APEC Privacy Subgroup, EU data protection Commissioners, and consumer groups, noted that although the Australian Privacy Foundation proposed better NGO input into APEC processes, 'other NGOs, meeting separately later in the week, are still concerned that engaging formally with the APEC process may be a trap that NGOs should avoid'.

In 2008 the civil society organisations are testing the strategy of engagement, to see if it yields any positive results. As noted, it has not yet yielded subgroup membership. However, at the February 2008 Privacy Subgroup meeting in Peru, three representatives of 'civil society' organisations[3] were invited to speak in the public seminar, and were allowed by their national delegations to support the membership applications at the Subgroup meeting. Even without formal guest status, the civil society organisations have been invited to participate in conference calls on the Pathfinder projects. All very well, but it is a bit late. In contrast, the subgroup Chair drafted the Pathfinder Work Plan in 2007 and noted that 'ICC had the opportunity to consider the draft and circulated some comments which identified areas where it is necessary to broaden the discussion in the document. There was discussion about the projects'. It is clear from this, and from its participation in all projects, that ICC uses its participation right aggressively to influence every aspect of the sub-group's work. Consumer groups were at that time shut out from such a level of participation. It is of less value to be allowed to participate once the principal rules have already been set.

Despite this progress, there is still too much of one rule for business, another for consumers. This is not sustainable if APEC's processes are to have long-term credibility. APEC's Privacy Subgroup needs to change from being a forum which is biased in favour of business interests to one which is more even-handed.

[3] Nigel Waters (Australian Privacy Foundation, representing Privacy International), Katitza Rodriguez (Electronic Privacy Information Centre (EPIC), USA) and Philippa Lawson (Canadian Internet Policy and Public Interest Clinic (CIPPIC))

Does APEC offer a future for privacy protection?

The APEC Framework is supposed to be agnostic as to which route(s) economies take to implement its Principles, whether the route is via binding corporate rules (BCRs), trustmarks, legislation or other means. But it is notable that, while there has been some belated recognition that enforceable remedies will be necessary, the Data Privacy Subgroup's workplan has never included anything expressly to do with supporting legislative development (such as seminars on options in drafting privacy laws to achieve different goals). It is now focused solely on developing a CBPR system. Waters (2008) notes that 'APEC has confirmed that the CBPR approach is only *one* way of implementing the APEC Privacy Framework, *albeit* currently the main focus of the Privacy Subgroup'.

When one of the principal drafters of China's proposed data protection gave details of what was then China's proposed Personal Information Protection Act (see Greenleaf, 2008a, 2008b) at APEC's public seminar in Canberra in January 2007, this attracted no public comment from anyone engaged in the APEC processes who was present. That one of the two giant economies of APEC was proposing to protect privacy by comprehensive national legislation almost seemed to be an embarrassment to APEC, even though it is the most direct route to complete compliance with the APEC Privacy Framework.

As a result, APEC often seems to be little more than a vehicle for advancing the interests of those business groups and economies that seem wish to deter and deflect as many countries as possible from adopting information privacy laws, and in particular from adopting any legally enforceable restrictions on exports of personal data. Until APEC gives the same priority to supporting both legislative and non-legislative developments, unambiguously accepts the rights of economies to have reasonable data export limitations, and gives the same status to consumer/privacy groups as it currently gives to business/surveillance groups, it is hard to see its Privacy Framework as having any significant positive effect on the development of privacy protection in the Asia-Pacific.

Of course, the APEC Privacy Framework and its processes could be more than they are at present. They could be a useful means of advancing information privacy protection in those Asia-Pacific countries where there is none of significance; of advocating a minimum standard of privacy Principles to be achieved by verifiable means; and of facilitating trans-border data flows within a framework of national laws. Europe has made significant progress toward these goals over 25 years, though there is still a long way to travel. The APEC process is showing little sign as yet that it is even pointed in the right direction.

Alternative futures for Asia-Pacific privacy

If APEC's Privacy Framework and its CBPR focus is not going to be the driver of major changes to privacy protection in the region, where are they going to come from. Three possible drivers are new national privacy laws, the region's privacy officials learning to act collectively, and (somewhat speculatively) the possibilities inherent in the Council of Europe Convention 108 as the basis for a global privacy Convention.

New national privacy laws?

A new wave of national legislation would make APEC less relevant, particularly if it is origins had little to do with APEC. The draft Chinese law that was under consideration seemed to fit that description (see Greenleaf 2008a, 2008b), but China's intentions are still a mystery. Chinese legislation would change the whole regional privacy equation, providing another model for emulation and a signal that privacy legislation is part of the package of a

modernising economy. ASEAN only has a partial overlap with APEC membership, and has recently had a significant emphasis on the drafting and enactment of e-commerce laws. A model ASEAN privacy law, drafted from the perspective of facilitating e-commerce, could lead in a new direction. Waters (2008) states that 'Peru, China, Thailand and the Philippines all reporting in Lima that they are well advanced with the introduction of an information privacy law'.

The limited vision of the Asia-Pacific's privacy Commissioners

As Stewart, Waters and others have suggested, collective judgments about compliance with regional privacy standards may eventually be inevitable, and it this occurs then it may require collective input from the region's privacy authorities.

European data protection Commissioners have a long history of collective deliberation, and in the last ten years, of collective action. The EU national Commissioners make up the Data Protection Working Party ('Article 29 Committee') established under the European privacy Directive (A29 Committee website), and as such have a formal role in deliberating on the adequacy of privacy laws of non-EU countries, as well as on many other matters of collective concern to privacy protection in Europe, and advising other European bodies on this. In their first decade they published 118 collective Opinions, Annual Reports and Working Documents since 1997. The Committee is generally regarded as among the world's most authoritative and influential voices on privacy issues.

There is as yet nothing similar in the Asia-Pacific. The Asia-Pacific Privacy Authorities Forum (APPA Forum), previously known as PANZA+, includes the data protection authorities of Australia (all jurisdictions with such), New Zealand, Hong Kong, South Korea and Canada (federal and British Columbia). To be an APPA member, authorities have to be accredited to the international meeting of Commissioners and come from Asia or the Western Pacific (Stewart, 2006). APPA and its predecessor bodies have met six monthly for fourteen years. APPA's Statement of Objectives (2005), other than being a general agreement to cooperate and exchange information, has its most concrete objective as 'Promoting best practice amongst privacy authorities'. In contrast, the 'Tasks of the Article 29 Data Protection Working Party' (A29 Committee, Tasks) is replete with substantive objectives, including 'To make recommendations to the public at large, and in particular to Community institutions on matters relating to the protection of persons with regard to the processing of personal data and privacy in the European Community.'

The severely limited collective role of the Asia-Pacific Commissioners is best appreciated by considering things it has not done. It has never issued a collective opinion on a privacy issue of regional or global importance, such as on particular privacy practices of global companies or on outsourcing practices. The Article 29 Committee has given many such opinions. It did not provide any collective input into the development of the APEC Privacy Framework, though individual offices from some jurisdictions (eg NZ, HK) were significant in the process.

There are both good reasons and excuses for the differences between Europe and the Asia-Pacific. The Europeans have more countries with privacy laws, and the A29 Committee has a formal collective role enshrined in a Directive which gives them a mandate to stick their collective noses into any privacy issue they think is important enough, and to do so publicly. One of the many failures of the process leading to the APEC Privacy Framework is that the creation of any such collective body of privacy authorities was not even on the agenda for discussion. The Asia-Pacific Commissioners have never had sufficient courage of their own

convictions to invent a role for themselves, possibly at risk of upsetting national governments. It would be possible to find sufficient mandate in the legislation of most in order to enable them to have some larger collective role: it is a question of will. Since 2005 APPA is becoming more organized and purposeful, but has not yet found a substantive role in the region's privacy protection.

The continuing influence of the EU privacy Directive

The European Union privacy Directive's (European Union, 1995) requirements concerning the 'adequacy' of the privacy laws of third countries before there can be unconditional exports of personal data to them from EU member states has taken a lot longer to 'bite' than many expected. There are a number of reasons for this. It has taken a long time for EU countries to bring their own laws into line with the Directive, and some still have not done so fully, to the extent that the European Commission is taking action against some of them. Individual EU countries have been reluctant to prevent data transfers to third party countries. The Commission has been very slow to complete its determinations of adequacy, or lack of it, for very many countries, no doubt being very reluctant to find non-EU countries' laws inadequate when so many EU laws were still so manifestly lacking.

There has as yet not been any finding that the laws of an Asia-Pacific country are not adequate. There has been a provision finding in favour of Canadian federal law, which is now being reviewed in the context of all Canadian jurisdictions. The US 'Safe Harbor' scheme, of very limited scope, was held adequate. A consultants' report to the Commission on all of Australia's laws has not progressed further as yet. The Commission is not know to have commenced any formal investigation of the laws of New Zealand, Hong Kong, Japan, Korea or Taiwan.

Slow though it is in maturing, the EU adequacy issue is not going to go away, and nor should it. The EU is not unreasonable in insisting that the privacy of Europeans whose personal data is being exported is provided adequate protection, and the Directive is quite flexible in how such protection can be achieved.

The attraction to countries in the Asia-Pacific of a blanket finding of 'adequate' for their laws will persist. The apaprent motivation behind some of the proponents of the APEC process to form an 'APEC bloc' that either explicitly rejected or ignored any European privacy standards (see Ford 2003, Crompton and Ford 2005) has not yet succeeded, as APEC has not established anything substantial of its own. The attraction of 'EU adequacy' is likely to persist over time and will influence many aspects of future Asia-Pacific privacy laws.

Conclusion: A two-tiered privacy system for the Asia-Pacific?

The world's privacy and data protection Commissioners at their 27th International Conference in Montreux, Switzerland agreed on a concluding 'Montreux Declaration' (2005) which issued a number of challenges to global organizations and national governments. One was their appeal 'to the Council of Europe to invite, in accordance with article 23 [of Convention 108 on data protection] … non-member-states of the Council of Europe which already have a [sic] data protection legislation to accede to this Convention and its additional Protocol.' Since 2001 a similar approach has seen the Council of Europe Cybercrime Convention become an international instrument with significant adoption outside Europe. The Commissioner's challenge signals a possible way of sidestepping the cumbersome process of developing a new UN convention on privacy, by starting with an instrument already adopted by the region with the most concentrated distribution of privacy laws, Europe.

This approach deserves serious consideration by Asia-Pacific governments which already have privacy laws of international standards (or are considering introducing same), and more academic analysis than is possible in the conclusion of this paper. It could provide a reasonable basis (a common reasonably high privacy standard) for a guarantee of free flow of personal information between parties to the treaty, both as between Asia-Pacific countries and as between those countries and European countries. Such invitation and accession would be likely to carry with it the benefits of a finding of 'adequacy' under the EU Directive, given that the 2001 Additional Protocol (CoE 2001) to the Convention has added a data export restriction and a requirement of an independent data protection authority to bring it more into line with the EU privacy Directive. Furthermore, the Directive allows a country's international obligations to be considered in determining the 'adequacy' of its laws.

Given that the APEC Privacy Framework has not attempted to provide such a general mechanism for free flow of personal information within the Asia-Pacific, perhaps globalizing this European instrument is now the realistic way open to do so. It would also be a much quicker solution than waiting for some new global enforceable treaty to emerge from the UN or elsewhere, or waiting for the EU's slow process of adequacy assessment to grind onward.

The result would be a two-tiered system of international data protection in the Asia-Pacific. For the first tier countries, membership of the Council of Europe Convention would guarantee free flow of personal information both between their Asia-Pacific peers who are also members, and with European countries. For the remaining countries ('economies'), APEC's Privacy Framework would provide a relatively low level of privacy protection to which economies with little or no existing protection could adopt by whatever means they chose, and a CBPR procedure which might give them some assistance in relation to data exports with similar economies or (with more difficulty), the countries that are also in the first tier. It would be an initiative which would allow all Asia-Pacific countries to move forward.

References

A29 Committee website <http://europe.eu.int/comm/justice_home/fsj/privacy/workinggroup/index_en.htm>

APEC (2007) – APEC Privacy Subgroup (submitted by Australia) *Pathfinder Project Outlines: Possible Pathfinder Projects for Cairns implementation*, <http://aimp.apec.org/Documents/2007/ECSG/SEM2/07_ecsg_sem2_003.doc>

APEC (2007a) – Concluding Senior Officials' Meeting (Submitted by: CTI/ECSG) *APEC Data Privacy Pathfinder* (2007/CSOM/019), <http://aimp.apec.org/Documents/2007/SOM/CSOM/07_csom_019.doc>

APEC (2007b) – Data Privacy Subgroup Chair *APEC Data Privacy Pathfinder: Proposed Work Plan*, Sydney, September 2007 <http://aimp.apec.org/Documents/2007/ECSG/ECSG2/07_ecsg2_008.doc>

APEC (2005) – Asia-Pacific Economic Cooperation (APEC) Privacy Framework - [2005] PrivLRes 4 < http://www.worldlii.org/int/other/PrivLRes/2005/4.html>

APEC (2004) - *APEC Privacy Framework*, November 2004 - Available from <http://www.apec.org/content/apec/apec_groups/som_special_task_groups/electronic_commerce.html> (PDF) (follow link); or in HTML from APEC drafts (2003-04) below

APEC drafts (2003-04) - for both the final Framework and some of the previous drafts see <http://www.bakercyberlawcentre.org/appcc/>

APEC ECSG Report (2005) - Report of the APEC Electronic Commerce Steering Group 11th Meeting, Seoul, Republic of Korea 24-25 February 2005 to the Senior Officers Meeting (2005/SOM I)

APEC ECSG Privacy (2005) – ECSG Data Privacy Subgroup Chair *Final Report of the 2nd Technical Seminar on APEC Privacy Framework*, ECSG Plenary Meeting, Gyeongju, Korea, 8-9 September 2005

APEC ECSG <http://www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce.html>

APEC Framework Part B - *APEC Privacy Framework International Implementation ("Part B")* Final – Version VII ECSG Plenary Meeting Gyeongju, Korea, 8-9 September 2005

APPCC (2004) - Asia-Pacific Privacy Charter Council *Submission to the APEC Electronic Commerce Steering Group Privacy Sub-Group* 31 May 2004 at <http://www.bakercyberlawcentre.org/appcc/APEC_APPCCsub.htm>.

Crompton and Ford (2005) – Malcolm Crompton and Peter Ford *Consultant's Issues Paper*, APEC Privacy Sub-Group, July 2005 (circulated to attendees at the first APEC Implementation Seminar; copy on file with author)

Council of Europe (1981) - Council of Europe *Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data* (Convention No 108) 1981 (Convention No 108)

Council of Europe (2001) - *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows*, Strasbourg,8.XI.2001, available at <http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm>

Ford (2003) - Ford, P 'Implementing the Data Protection Directive - An Outside Perspective' [2003] 9 PLPR141

Greenleaf (2008) – Greenleaf, Graham 'APEC's privacy Pathfinders – a dead end for consumers?' *Privacy Laws & Business International Newseletter*, Issue 91, February 2008

Greenleaf (2008a) – Greenleaf, G 'China's proposed Personal Information Protection Act (Part I): The principles' *Privacy Laws &Business International Newsletter*, Issue 91, February 2008

Greenleaf (2008b) – Greenleaf, G 'Enforcement aspects of China's proposed Personal Information Protection Act' *Privacy Laws & Business International Newseletter*, Issue 92, April 2008

Greenleaf (2007) – Greenleaf, G 'Asia-Pacific developments in information privacy law and its interpretation' [2007] UNSWLRS 5 (bepress); presented at *Privacy Issues Forum*, Wellington NZ, 30 March 2006

Greneleaf (2005e) – Greenleaf, G 'APEC Privacy Framework completed: No threat to privacy standards', *Privacy Laws &Business International Newsletter*, Issue 79, Sept/Oct 2005

Greenleaf (2005d) – Greenleaf, G 'Implementation of APEC's Privacy Framework' in Datuk Haji Abdul Raman Saad Personal (Ed) *Data Protection in the New Millenium*, LexisNexis, Malaysia, 2005

Greenleaf (2005c) – Greenleaf, G 'APEC's Privacy Framework sets a new low standard for the Asia-Pacific' in M Richardson and A Kenyon (Eds) *New Dimensions in Privacy Law: International and Comparative Perspectives,* Cambridge University Press

Greenleaf (2005) - Greenleaf, G 'APEC's Privacy Framework: A new low standard' (2005) *Privacy Law & Policy Reporter* Vol 11 Issue 5

Greenleaf (2004) - Greenleaf, G f 'APEC's privacy standard regaining strength' (2004) 10(8) PLPR 158

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

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

Greenleaf (2003c) - Greenleaf, G 'APEC privacy principles: More Lite with every version' (2003) 10(6) *PLPR* 105

HK Seminar (2005) - Website for at the first *APEC Electronic Commerce Steering Group (ECSG) Technical Assistance Seminar: Domestic Implementation of the APEC Privacy Framework,* Hong Kong, June 2005, located at <http://www.pco.org.hk/english/infocentre/apec_ecsg1_2.html.>

Kirby (1999) - Justice Michael Kirby 'Privacy protection, a new beginning: OECD principles 20 years on' (1999) 6 PLPR 25

Lawson (2007) – Lawson, P 'APEC provides second class privacy protection', *Privacy Laws &Business International Newsletter*, Issue 89, October 2007, pgs 13-14

Montreux Declaration (2005) - 'The protection of personal data and privacy in a globalised world: a universal right respecting diversities', Declaration of the 27th International Conference of privacy and Data Protection Commissioners, Montreux, Switzerland, September 2005

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

Stewart (2005) - Blair Stewart, Assistant Privacy Commissioner, New Zealand 'Mechanisms for reporting on domestic implementation' (at HK Seminar (2005))

Waters (2007) – Waters, N 'NGO view of DP Commissioners' Conference, Montreal' *Privacy Laws &Business International Newsletter*, Issue 90, December 2007, pgs 12-13

Waters (2008) – Waters, N 'NGOs 'cautious optimism' on APEC privacy initiative' *Privacy Laws &Business International Newsletter*, Issue 92, April 2008 (in publication)