University of New South Wales
University of New South Wales Faculty of Law Research Series

Year 2007 *Paper* 5

Asia-Pacific Developments in Information Privacy Law and its Interpretation

Graham Greenleaf*

*University of New South Wales

Asia-Pacific Developments in Information Privacy Law and its Interpretation

Graham Greenleaf

Abstract

It is easy to be preoccupied with our domestic information privacy laws to the exclusion of the international context in which they operate and the international forces on their formation and implementation. In this paper I provide a brief survey of the main international agreements and institutions currently influencing the development and operation of information privacy laws in Asia-Pacific countries. I suggest that Asia-Pacific Privacy Commissioners are yet to achieve a significant enough collective role; that the UN is largely irrelevant to the future of privacy protection; that the APEC Privacy Framework is a missed opportunity for a meaningful regional privacy agreement; and that it is now potentially useful for less developed countries provided a careful eye is kept on the role of the US and its privacy allies; that we need to better understand the interpretation of privacy principles by Courts, Tribunals and Commissioners so as to develop an Asia-Pacific privacy jurisprudence, and that our best hope for some type of meaningful international standard may be (strange as it seems) for Asia-Pacific countries to join the Council of Europe privacy Convention.

Asia-Pacific developments in information privacy law and its interpretation

Professor Graham Greenleaf
University of New South Wales
<http://www2.austlii.edu.au/~graham>

A background paper prepared for the ***Privacy Issues Forum***, 30 March 2006, Museum of New Zealand – Te Papa Tongarewa, Wellington, hosted by the New Zealand Privacy Commissioner[1].

Contents

---

[1] *Please note*: An earlier version of parts of this paper was presented as G Greenleaf 'The global context of privacy rights policies in the digital age: Prospects and present situation', pgs 69-99, in *(Proceedings) International Forum on Privacy Rights in the Digital Age*, September 2005, Korean National Commission for UNESCO, Seoul, South Korea, available at <http://www2.austlii.edu.au/~graham/publications/2005/UNESCO_Privacy.html>. Some material on the APEC Privacy Framework in this paper is derived from book chapters by the author: 'Implementation of APEC's Privacy Framework' in Datuk Haji Abdul Raman Saad Personal (Ed) *Data Protection in the New Millenium*, LexisNexis, Malaysia (forthcoming, 2005); and '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 (forthcoming, 2006).

International influences on privacy law in the Asia-Pacific

It is easy to be preoccupied with our domestic information privacy laws such as New Zealand's *Privacy Act 1993* and Australia's *Privacy Act 1988*, to the exclusion of the international context in which they operate and the international forces on their formation and implementation.

More accurately, it is easy to do so in the minority of countries that have such laws. In the Asia-Pacific we can count on that hand Australia, Canada, Hong Kong, New Zealand, South Korea, and Japan (though weak and untested), as having relatively comprehensive laws, and Taiwan, Thailand and the United States as having partial coverage.

In this paper I provide a brief survey of the main international agreements and institutions currently influencing the development and operation of information privacy laws in Asia-Pacific countries. I suggest that Asia-Pacific Privacy Commissioners are yet to achieve a significant enough collective role; that the UN is largely irrelevant to the future of privacy protection; that the APEC Privacy Framework is a missed opportunity for a meaningful regional privacy agreement; and that it is now potentially useful for less developed countries provided a careful eye is kept on the role of the US and its privacy allies; that we need to better understand the interpretation of privacy principles by Courts, Tribunals and Commissioners so as to develop an Asia-Pacific privacy jurisprudence, and that our best hope for some type of meaningful international standard may be (strange as it seems) for Asia-Pacific countries to join the Council of Europe privacy Convention.

Privacy Commissioners acting collectively

The Montreaux Declaration 2005 – A challenge by the world's privacy Commissioners

The annual meetings of the world's privacy and data protection Commissioners are not noted for their startling declarations or plans of action, but at their 27th International Conference in Montreux, Switzerland in September 2005, they agreed on a concluding 'Montreux Declaration' which issues a challenge to global organizations and national governments (Montreux Declaration 2005).

In their final communiqué, after noting complexities of 'the current geopolitical context, and in particular the war on terrorism, the internet, biometrics, the development of invasive technologies and the appearance of biobanks', the Commissioners summed up their Declaration as follows,

> "In order to confront these challenges, the commissioners have agreed to work towards a recognition of the universal nature of data protection principles. At Switzerland's initiative, they adopted a final declaration in which they committed themselves to work with governments as well as international and supranational organisations with a view to adopting a universal convention on data protection. The declaration appeals in particular for:
>
> - the UN to prepare a binding legal instrument
> - governments to encourage the adoption of legislation in line with recognised data protection principles and to extend it to their mutual relations

- the Council of Europe to invite non-member states of the organisation to ratify the Convention for the protection of individuals with regard to automatic processing of personal data and its additional protocol

- to Heads of States and Governments that will join in Tunis for the World Summit on the Information Society (16-18 November 2005) to include in their final declaration a commitment to develop or reinforce a legal framework that ensures the rights to privacy and data protection to all citizens within the Information Society

- international and supranational organisations to commit themselves to complying with data protection rules

- international non-governmental organisations to draw up data protection standards

- hardware and software manufacturers to develop products and systems that integrate privacy-enhancing technologies."

They propose that progress in implemention will be subject to regular assessment.

What is the 'the universal nature of data protection principles' that the Montreux Declaration assumes? The Declaration states that these principles 'derive from international legal binding and non-binding instruments such as' the OECD Guidelines, the Council of Europe Convention, the UN Guidelines, the EU Directive and the APEC Framework (para 16). It then states that 'these principles are in particular the following' (para 17) and lists the nine apparently standard headings for the content of information privacy principles ('Principle of lawful and fair data collection and processing' etc), plus two Principles which go to enforcement: 'Principle of independent supervision and legal sanction' and 'Principle of adequate level of protection in case of transborder flows of personal data'.

While the nine headings of the content principles are too vague for any conclusions to be drawn as to the detailed substance of the privacy principles that might obtain worldwide consensus by privacy Commissioners, the two principles of enforcement and more concrete and significant. Taken at face value, all of the world's privacy Commissioners, including those from the Asia-Pacific, are calling on the UN and governments to accept that information privacy principles must be enforced by legal sanctions, and must be under the supervision of an independent body. Furthermore, there seems to be an acceptance that transborder flows of personal data should only occur under conditions of adequate protection.

These recommendations may not seem startling, but they are a stronger statement of the requirements of privacy protection than are made by the APEC Privacy Framework, or have yet been made by the privacy Commissioners of the Asia-Pacific by themselves. They are therefore significant to our region as the strongest statement by privacy 'officials' relevant to us.

Regional roles - Asia-Pacific vs European Commissioners

European data protection Commissioners have a long history of collective deliberation, and in the last ten years, of collective action. What is now the international annual meeting of privacy Commissioners started as a European meeting. 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. They are supported by a Secretariat at the European Commission. They have published via their website 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, perhaps the most authoritative from any normative perspective.

There is as yet nothing resembling this body 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 and South Korea. 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's achievements include 24 meeting over 14 years, now six monthly. No doubt newly-established offices have received valuable advice from those longer established. APPA adopted a Statement of Objectives (see Appendix 1) at its formation in 2005, but other than being a general agreement to cooperate and exchange information its most concrete objective is '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.' APPA has also adopted a standard for case citations, which its European counterpart has not done.

However, the severely limited collective role of the Asia-Pacific Commissioners to date 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 were significant in the process in countries (such as New Zealand) where the government did not exclude them from the process (such as Australia). It is invisible to the general public and to most of the informed public and does not even have its own website yet.

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 they have 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. Any such move would have been vigorously opposed by the USA. 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 privacy authorities. It would not be difficult to find sufficient mandate in the legislation of most in order to enable them to do so: it is a question of will.

Since 2005 APPA is becoming more organized and purposeful, but we must wait and see whether it finds a substantive role in the region's privacy protection.

The minor roles of the UN in global privacy protection

The Privacy Commissioners at Montreaux called on the UN to develop 'a binding legal instrument which clearly sets out in detail the rights to data protection and privacy as enforceable human rights'.

Does the progress that the UN made on privacy protection in the past give us any reason to expect it might rise to this challenge? The answer must be 'no', as explained in the following paragraphs: there is little chance of the A17 privacy rights in the International Covenant on Civil and Political Rights becoming enforceable in many Asia-Pacific countries or developing a significant privacy jurisprudence; the UN's 1990 Guidelines Concerning Computerized Data Files have been ignored; and the 2003-05 World Summit on the Information Society produced nothing of significance concerning privacy.

The UN Human Rights Committee and interpretations of A17 ICCPR

At the 1998 UNESCO symposium considering privacy in the information society, Marc Rotenberg of EPIC observed that 'core privacy principle in modern law' (Rotenberg, 1998) is the *Universal Declaration of Human Rights* 1948 Art 12, which states 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks'. Provisions with similar wordings are now found in the International Covenant on Civil and Political Rights 1966 (ICCPR) A 17; American Convention on Human Rights (ACHR) 1969, A 11, and the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) A8.

From these various treaties, the most sophisticated privacy jurisprudence has been developed by the European Court of Human Rights in relation to A8 of the ECHR (see Bygrave 1998 for analysis). The UN Human Rights Committee (UNHRC) is only able to interpret and apply A17 in relation to complaints ('communications') it receives from individuals against those States that are parties to the First Optional Protocol to the ICCPR, granting the Committee jurisdiction to receive communications.

There are very few cases that have come before the UNHRC concerning privacy and A 17. The handful of significant cases include:

- *Toonen v Australia* [1994] UNHRC 9 – The law of an Australian State criminalised all sexual contact between consenting male adults in private, UNHCR held Australia in breach of A17. The law was changed.

- *Coeriel and Aurik v Netherlands* [1994] UNHRC 56 - Refusal to allow change of names to Hindu names (necessary for study for priesthood) was a privacy breach of A17.

- *Hopu and Bessert v France* [1997] UNHRC 40: The UNHRC concluded 'that the construction of a hotel complex on the authors' ancestral burial grounds did interfere with their right to family and privacy. The State party has not shown that this interference was reasonable in the circumstances…'

The privacy jurisprudence of the UNHRC has therefore been rather peripheral to the core issues of protection of privacy in the information economy. It remains to the seen whether the new UN human rights body being formed will make any difference.

Furthermore, of over 100 countries to have ratified the 1st Optional Protocol, the only Asia-Pacific countries to have done so are Australia, Canada, New Zealand and South Korea, with Sri Lanka the only other country nearby.

It appears therefore that the existing UN structure has little prospect of development as a significant part of global privacy protection.

The UN Guidelines concerning Computerized Personal Data Files

Guidelines Concerning Computerized Data Files were adopted by the UN General Assembly on 14 December 1990, having been previously adopted by the Human Rights Committee. They arose from a French initiative. The voluntary guidelines contain minimum standards for incorporation in national legislation, covering such matters as collection, accuracy, purpose specification, access, non-discriminatory use, security, trans-border data flows, supervision and penalties. At the 1989 Data Protection Commissioner's Conference a number of Commissioners expressed the hope that the UN initiative would facilitate the spread of privacy legislation beyond Europe and North America, which did not happen. The Montreux Declaration is to some extent a continuation of that wishful thinking by Privacy Commissioners, and its calls on the UN will almost certainly be ignored.

The UN WSIS – Largely ignoring privacy

The World Summit on the Information Society (WSIS, 2005) comprised two meetings (Geneva in 2003 and Tunis in 2005) dealing with information society issues, making up one summit. As far as privacy is concerned, they did not amount to much except that privacy was not totally ignored in favour of security interests.

Geneva 2003

The Declaration of the first meeting (WSIS Declaration, 2003) says very little about privacy. The section on 'Building confidence and security in the use of ICTs' (B5) treats privacy as part of 'cyber-security' and states (italics added):

> 35. Strengthening the trust framework, including information security and network security, authentication, *privacy* and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs. A global culture of cyber-security needs to be promoted, developed and implemented in cooperation with all stakeholders and international expert bodies. These efforts should be supported by increased international cooperation. Within this global culture of cyber-security, it is important to enhance security and to ensure *the protection of data and privacy*, while enhancing access and trade. In addition, it must take into account the level of social and economic development of each country and respect the development-oriented aspects of the Information Society.

Spam is recognized as 'a significant and growing problem for users, networks and the Internet as a whole' but is considered in the context of cyber-security with no specific mention of its privacy-invasive effects (para 37). .

The section on 'Ethical dimensions of the Information Society' (B10) states:

> 58. The use of ICTs and content creation should respect human rights and fundamental freedoms of others, *including personal privacy*, and the right to freedom of thought, conscience, and religion in conformity with relevant international instruments.

These two slight mentions are all the WSIS Declaration has to say about privacy.

Bendrath (2005) explains that in 2003 the summit was dominated by discussions of cyber-security and preventing ICT networks being used to aid terrorism, and 'in this context, the protection of privacy was not a popular goal'. The first drafts of the WSIS Declaration made no mention of privacy at all, and it was only later mentioned 'due to the efforts of the European Union, Switzerland, Brazil, Australia and a few other countries'.

Considerable efforts by the international NGO network active in the WSIS process (the Privacy and Security Working Group and the Human Rights Caucus) to have a separate paragraph on privacy included were not taken up by any of the state delegations. The paragraph they proposed would have read:

> The right to privacy is a human right and is essential for free and self-determined human development in the knowledge society. Respect for privacy allows for both participation and detachment in regard to social activities and opportunities. Every person must have the right to decide freely whether and in what manner he/she wants to receive information and communicate with others. The possibility of receiving information anonymously, irrespective of the source, must be ensured for everyone. The power of the private sector and of governments over information increases the risk of manipulative access and surveillance and must be kept to a legally legitimised minimum. The collection, analysis and release of personal data – no matter by whom – should remain under the control of the individual concerned.

This paragraph is derived from the *Charter of Civil Rights for a Sustainable Knowledge Society* developed by German civil society groups and adopted by other civil society organizations at the WSIS meeting (see .Jorgensen 2003 and Kuhlen 2003).

Tunis 2005

The Privacy Commissioners in their Montreux Declaration called on governments at the Tunis WSIS 'to include in their final declaration a commitment to develop or reinforce a legal framework that ensures the rights to privacy and data protection to all citizens within the information society'. They note that summit meetings of heads of government of both the Spanish-speaking and French-speaking worlds have made such commitments (Summit of Santa Cruz, 2003, and Summit of Ougadougou, 2004, respectively). No such declaration has been made by a summit of APEC leaders or other leaders in the Asia-Pacific region, and the APEC Privacy Framework does not constitute an agreement to develop a *legal* framework.

The Second WSIS 2005 summit in Tunis produced little better result in relation to privacy than the first. The 'Tunis Commitment' (WSIS 2005) made no mention of privacy beyond endorsing what was said in Geneva. The *Tunis Agenda for the Information Society* (WSIS 2005) contains a vague endorsement of protection of information privacy but by no particular means:

> "46. We call upon all stakeholders to ensure respect for privacy and the protection of personal information and data, whether via adoption of legislation, the implementation of collaborative frameworks, best practices and self-regulatory and technological measures by business and users. We encourage all stakeholders, in particular governments, to reaffirm the right of individuals to access information according to the Geneva Declaration of Principles and other mutually

> agreed relevant international instruments, and to coordinate internationally as appropriate."

Other paragraphs call for respect for privacy in moves to strengthen network security (para 39) and in the fight against spam (para 39).

It seems therefore that in the current world climate, getting the UN to focus on the need for a global standard for privacy protection will not be an easy task, and may not be worth attempting.

APEC's Privacy Framework: A missed opportunity?

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 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). For the reasons set our below this is unlikely to be the case, though it may well have some positive effects. However, compared with its potential, the actuality 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' includes Section A 'Guidance for Domestic Implementation' did not include Section B on the 'cross-border elements' (including data exports). In September 2005 Part IV(B) was added and the Framework completed.

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. And yet, some business groups and governments are extremely enthusiastic about it (BNA 2006). To paraphrase Mandy Rice Davies (1963), 'well, they would be, wouldn't they?'

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. The definition does not cover information which may be used to transact with an individual (eg phone numbers, email addresses and IP addresses), even though their identity may not be known. Other laws and agreements don't cover this aspect either, but this illustrates where APEC's principles reflect the past and do not deal with present and future problems. '*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' (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.

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

I Preventing Harm

The sentiment that privacy remedies should concentrate on preventing harm ('should be designed to prevent the misuse of such information' and 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 (eg small business in Australia's law) as not sufficiently dangerous, 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 regional laws). 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 regional laws 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 regional laws.

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 regional laws 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 '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 (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).

APEC Privacy Principles - Five bases for criticism

There are five distinct forms of criticism that may be leveled at the APEC IPPs, which I have developed at greater length elsewhere (Greenleaf, 2005a), and are inherent in my above outline of the Principles.

(1) ***Weaknesses inherent in the OECD Principles*** First, the APEC IPPs 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.

(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 IPPs improve on some OECD IPPs in minor ways, and they are weaker than others in some ways. They do not include the OECD IPPs 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. Examples given below are 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. 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 IPPs which go beyond those of the OECD, and very often share these new IPPs 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 regional and other Principles are 'missing' from APEC?

To demonstrate the essentially timid and backward-looking nature of the APEC principles, it is useful to consider what is missing. The following list gives some examples of distinct additional Principles that have developed in the 20 years since the OECD Guidelines, and are found in more than one of the existing regional privacy laws, and can therefore be said to have become (at least to some extent) a 'standard' that APEC has ignored or rejected. Also considered are principles contained in the OECD Guidelines themselves, or in the EU privacy Directive (and therefore all EU laws), or in the Asia-Pacific Telecommunity's Privacy Guidelines (APT 2003)

(i) ***Openness*** The OECD Openness Principle's requires a 'general policy of openness about developments, practices and policies with respect to personal data' and that 'means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use'. These rights apply to any persons, not only data subjects in relation to their own data, and so are rights which are not covered by APEC's Notice Principle or its right of access. They are important rights to ensure openness of surveillance systems to public scrutiny. Openness principles are found in all Australian jurisdictions, Canada and HK. APEC has no equivalent.

(ii) ***Collection from the individual*** – Existing regional Acts require in different ways that collection of personal information should be from the individual concerned, wherever

possible, including Canada, Australian privacy sector, NSW, Vic, NT and NZ. APEC has no equivalent.

(iii) ***Data retention*** A 'limited retention principle', initially supported by New Zealand, Hong Kong, China and Taiwan, was removed by consensus from APEC consideration around draft 8. Some form of such a principle is found in HK, NZ, NSW, and Korea. Why should IPPs allow the unlimited retention of all personal information after it has ceased to have any continuing use to the retaining organisation?

(iv) ***Third party notice of corrections*** A right to have recipients of incorrect information informed of corrections is found in the jurisdictions of NSW, NZ and HK, and the EU, and the Australian Privacy Commissioner has recommended its inclusion in Australian federal law (APC, 2005). APEC has no equivalent.

(v) ***Data export limitations*** Restrictions on personal data exports to places where privacy laws are deficient are already found in the jurisdictions of Québec, Taiwan, HK (not yet in force), Australia (private sector NPPs), Victoria, Northern Territory, and NSW (not yet in force), as well of course as in the EU. The OECD Guidelines also acknowledged the legitimacy of such restrictions, as discussed below.

(vi) ***Anonymity*** – A right to have transactions remain anonymous where appropriate and practical is already found in the jurisdictions of Australia (private sector NPPs), Victoria, Northern Territory, and NSW (health privacy). The APEC Principles, it will be recalled, do not even contain a 'minimum collection' principle, and it would be difficult to argue for anonymity merely from the principle that information collected should be relevant to the transaction.

(vii) ***Identifiers*** APEC does not have a principle dealing specifically with limits on the sharing of identifiers. This is found in Australia's private sector NPP 7, Victoria and NT and in NZ's law.

(viii) ***Automated decisions*** The EU Directive provides that an organisation must not make a decision adverse to an individual based on automated processing without a prior review of that decision by a human (A15.1), and the APT has principles to similar effect. No regional laws yet have such a principle although the notice and challenge requirements in the data matching controls in the NZ and Australian privacy laws go some way in this direction .

(ix) ***Sensitive information*** The OECD Guidelines 'Part One - General' recognize that there may be a need for greater protection of sensitive classes of data (OECD 3(a)). IPPs providing protection for defined classes of 'sensitive' information are found in the privacy laws of Australia's private sector, Victoria, the NT and the EU.

(x) ***Public register principles*** APEC's definition of 'publicly available information' places no limits on the collection of information from public registers and its subsequent use (but not disclosure). Various regional privacy laws either apply their IPPs to public registers (eg HK) or include separate special 'public register principles' (eg NZ, NSW, Victoria)

APEC's domestic implementation – Exhortations without substance

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 does 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.'

What criteria are to be used to measure whether a chosen implementation measure is sufficient to implement the APEC IPPs? 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'. Legislation is mentioned as one means of providing remedies but is not required or even recommended (V). No external means of assessment are suggested.

The value of complainants having a choice of remedies is mentioned:

> "the importance of having a range of remedies commensurate with the extent of the actual or potential harm to individuals resulting from such violations" (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.

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).

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).

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, and

(as yet) no detailed criteria for development of an IAP (though development started at the second Implementation Seminar).

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. The APEC Framework is therefore considerably weaker than any other international privacy instrument in terms of its implementation requirements.

APEC's approach to data exports

OECD and EU approaches to data export issues – allowing and requiring

In the OECD Guidelines 'Part 3 - Basic Principles of International Application', guideline 17 explicitly sets out three situations when data export restrictions are acceptable: where the importing country does not 'substantially observe' the OECD Guidelines; country does not have its own data export prohibitions); and to protect sensitive data not similarly protected overseas.

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 allow (but do not require) data export restrictions to countries which do not 'substantially observe' the Guidelines.

The novel, perhaps revolutionary, development in the EU Directive was, 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 therefore nothing unusual an international privacy agreement being (in part) a guarantee to 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), and even making such restrictions mandatory (EU Directive).

The APEC Framework's approach – ignoring?

What approach is APEC taking to these issues? It is still not completely clear.

At the time of release of the 2004 Framework, it seemed possible that the Framework (via the missing Part IV (B)) might seek 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 limitations. A number of factors supported such an expectation:

- The Framework has frequent references to the 'essential' nature of free flows of personal information, amounting to 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..
- Even though the Framework could not 'require' any APEC member to allow data exports to other APEC members who (in some yet-to-be-specified way) implement

the Framework, a strong statement in the Framework that data exports should be allowed in certain circumstances would be very influential and treated as a requirement for 'compliance'. APEC agreements are not treaties and APEC does not usually attempt to require its members to take particular steps, but voluntary compliance would still be compliance.

- 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 international privacy instruments (as outlined above). So it would not be surprising *in principle* if the APEC Framework attempted to prevent data export restrictions within APEC provided the Frameworks standards were 'met'.

- Embodying such a 'trade-off' in the Framework was suggested by then APEC Sub-group Chair Peter Ford in his original *Privacy Implementation Mechanisms (Version 1)* accompanying version 1 of the APEC principles (APEC drafts, 2003-04). He proposed various types of self-certification mechanism for assessing whether Members Economies had implemented the Principles, and that such certification 'would be accepted by other economies as a basis upon which personal information could be transferred across national borders (see Greenleaf, 2003a). New Zealand's Assistant Privacy Commissioner distributed a paper in reply proposing external measures of assessing compliance (Stewart, 2003, discussed in Greenleaf, 2003a and Greenleaf 2005d). These proposals were not taken further at the time, but there was some expectation that they would re-emerge.

However, such expectations have not been borne out. Following the Second APEC Implementation Seminar in Kyongju, Korea, in September 2005, the Privacy Sub-Group recommended and obtained formal endorsement of the 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).

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

(i) Forbid 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 countries that have APEC-compliant laws (or equivalent protections) (contrast any other international privacy agreement).

The APEC Privacy Framework is therefore extremely non-prescriptive in relation to data exports, consistent with its general non-prescriptive nature. This rather benign result 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. Even though APEC has no such requirements of its own, it does not attempt via the formal terms of the Framework to prevent its member economies having data export restriction rules, whether for domestic privacy protection purposes or so as to meet to the EU's 'onward transfer' requirements.

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) prepared for the second seminar. The consultants propose 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.' The final version is consistent with this proposal of the APEC consultants, but does not goes as far as the tenor of the rest of their remarks suggest, which would have at least involved discouraging APEC economies from adopting data export restrictions. Such discouragement is not found in the APEC Framework, and nor is it found in the official Report on the second seminar (APEC ECSG Privacy 2005). Whether export restrictions will be discouraged in future APEC implementation seminars is another question, but it is not found in the words of the Framework itself.

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 considering action against some German jurisdictions for failure to have an independent data protection authority. 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 some 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 but that is now being reviewed. Consultants have presented a report to the Commission on all of Australia's laws, but that has not progressed further as yet. The Commission has not 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 ideological motivation behind some of the proponents of the APEC process, particularly those in Australia and the USA, 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 succeed in fashioning APEC into any such thing. It will probably fail to do so, and the attraction of 'EU adequacy' will persist over time and will influence many aspects of future Asia-Pacific privacy laws.

Some ways ahead for privacy principles in the Asia-Pacific

What lessons can we learn for the future development of privacy principles in the Asia-Pacific? I'd like to conclude with some observations on the directions it would be valuable to take from here.

The value of the APEC Framework, and its dangers

The was previously a danger that the missing Part IV(B) would turn APEC into a bloc which 'required' (in the weak APEC sense) personal data exports to countries which met a low standard of privacy principles and almost non-existent standard of implementation. The final version of the APEC Privacy Framework provides no formal basis for this to occur. The danger of an APEC that rejected data export limitation *en bloc* in confrontation with Europe is also largely removed.

As a result, the APEC process, despite the weakness of its Principles and its implementation, can be appreciated and encouraged for its positive potential even by civil society and other critics (such as the author) who regard the process and its outcomes as a lost opportunity of a higher and more genuine regional standard. If the APEC implementation process encourages countries that have no privacy laws to adopt them, even if a relatively low standard is adopted, then individuals in those countries will still benefit by better protection of their human rights.

The fact that, within a year of the Framework being adopted, APEC's implementation seminars have involved every significant county in APEC (except Malaysia) attending one or both of two two-day implementation seminars to discuss privacy issues is a notable achievement in itself. The seminars themselves have been biased in favour of business participation over that of civil society input, but that could be remedied in future.

However, dangers persist. While APEC's principles provide a modest statement of international privacy standards, its implementation and data export provisions provide no standards at all. There is a risk that the APEC implementation processes to 'educate' other APEC countries ('capacity building') will focus almost entirely on mechanisms for approving (or more accurately, not impeding) free flow of personal information, irrespective of how low the protections provided by the importing country may be. This can best be countered by the most positive of approaches: by countries (and NGOs) that value high standards of privacy protection insisting on a management role in the APEC implementation processes, and refusing to leave this to the USA and Australia.

Going beyond APEC – real regional standards

Since the APEC Framework does not claim that its Principles are the highest standard of privacy protection that should be adopted, there is room within the APEC privacy process for advocacy of the adoption of higher standards, based on the experience of other Asia-Pacific countries and that of Europe. Forums and tools are needed through which countries newly considering adopting privacy protection can learn of alternative models and experience. Those forums and tools should not be controlled by those who dominate the APEC process, given that they have settled on a rather lowest-common-denominator and business-dominated approach.

An Asia-Pacific privacy jurisprudence?

Irrespective of what normative position one takes on the question of how high privacy standards should be, there is a more basic need for international understanding in the Asia-

Pacific. The problem is that we do not have a good understanding of what most of our national laws mean, because there is such a paucity of case law of any type interpreting them. New Zealand is an exception, with a considerable body of law from the decisions of the Human Rights Review Tribunal. In Australia there has only been one court decision of any substance concerning the federal Privacy Act 1988, after 17 years. In Hong Kong the significant court decisions can be counted on a few fingers. Australia's federal Commissoner publishes less than 20 complaint summaries per year, in Hong Kong the number is under 10 per year, and in New Zealand the average is about 12 per year but this has declined only a handful in the last two years.

With at least ten privacy principles (depending on how you count them) requiring interpretation, these numbers are not going to provide an abundance of privacy case and complaint examples for any jurisdiction in the near future.

A potential answer lies in the similarities of the sets of principles, and 'core concepts' found in each jurisdiction's information privacy laws, particularly those in the Asia-Pacific. European laws have departed somewhat in a direction of their own, under the influence of the European privacy Directive. However, are these similarities of principles – and the resulting promise of the interpretations of one jurisdiction's laws being relevant to other jurisdictions – superficial but misleading, or are they real?

At this stage we don't know, but it seems a worthwhile enterprise to investigate the case law and complaints examples of the various Asia-Pacific jurisdictions systematically in order to compare how each principle and core concept is similar between jurisdictions, and then to what extent the case and complaints experience is in fact the interpretation and elaboration of a common body of legal principles. To some extent as yet uncertain, an Asia-Pacific information privacy law jurisprudence should emerge from such an investigation. It can then be taken further by searching for commonality with the European experience in interpreting their laws, given the common roots of both European and Asia-Pacific laws in the OECD privacy Guidelines (OECD, 1981).

Such a research project is now underway, the *interpreting Privacy Principles* (iPP) Project, based at the Cyberspace Law & Policy Centre at the University of New South Wales (see iPP website). Funded by the Australian Research Council for 2006-08, the lead investigators will be me, Paul Roth (Otago), and Lee Bygrave (Oslo), with Nigel Waters as principal researcher. The project will also have the equivalent of one full time research assistant.

Tools for learning from experience: Asia-Pacific case-law

One of the most important tools by which all jurisdictions can learn which aspects of other jurisdictions' privacy laws provide real remedies in concrete instances affecting real people is the reported cases from other jurisdictions. The principal research tool which will be developed by the iPP Project is the databases of the *Privacy Law Project* <http://www.worldlii.org/int/special/privacy/> on the World Legal Information Institute (WorldLII) website. It has already been in operation as a prototype for three years, but without any ongoing staff support. The Project's databases already include 19 databases of the texts of both adjudicated and mediated privacy disputes heard by Privacy Commissioners (and similar bodies), Tribunals and Courts, from Australia, Canada, Hong Kong, New Zealand, South Korea and some European countries, plus archives of the issues of three privacy journals and newsletters. It allows all databases to be searched together, and ranks cases found by likely relevance. The Project's databases already contain well over 1,000 privacy cases, plus many more cases on access and correction of personal information

under freedom of information laws, and we expect these numbers to double in a short time. It therefore provides most of the available case law experience from the Asia-Pacific. It was used by the APEC consultants to find their case studies for the first APEC implementation seminar.

The case databases in the Project will be augmented by databases of privacy legislation from around the world (initially that already available from free access Legal Information Institutes), and (on a similar basis) databases of international agreements and law reform reports dealing with privacy. Å great deal of relevant material on a particular core concept or privacy principle will then be retrievable.

The Privacy Commissioners' Montreux Declaration states that they agree 'to create a permanent website … as a common base for information'. Insofar as such a website would provide a means of comparing how different jurisdictions deal with common privacy issues, the *Privacy Law Project* goes some distance to providing such a facility, at least for the Asia-Pacific.

Harnessing civil society input

By the Montreux Declaration the Privacy Commissioners also agree 'to promote the exchange of information with international Non Government Organisations which are dealing with data protection and privacy'. The Asia-Pacific Privacy Commissioners (excluding the Canadians), meeting as PANZA+, have not made any effort to engage collectively with civil society organizations. The APEC Privacy Sub-group has been very effective in doing this with business NGOs, but has made little to no effort to do so with consumer, civil liberty and privacy NGOs. Since a significant amount of expertise in privacy issues is found outside the government sector in Asia-Pacific countries, this is unfortunate.

One difficulty is identifying appropriate NGOs at a regional level. The most active and effective NGOs are found at national level. The Asia-Pacific Privacy Charter Council (APPCC) was formed in 2003 as 'a regional expert group which will develop independent standards for privacy protection in the region, in order to influence the enactment of privacy laws in the region in accordance with those standards, and the adoption of regional privacy agreements in accordance with those standards'. The Council, which has expert members from ten countries in the region (see APPCC 2003), has not yet released any draft Asia-Pacific Privacy Charter, but was the only organisation to make a critical submission to the APEC Privacy Sub-group on the draft APEC Privacy Principles.

Sidestepping the UN and APEC via the Council of Europe Convention?

In the Montreux Declaration the Commissioners appeal 'to the Council of Europe to invite, in accordance with article 23 of the Convention … 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 of widespread adoption outside Europe. It is a 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.

This approach deserves serious consideration by Asia-Pacific Privacy Commissioners and governments, as 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 likely 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.

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.

What can APPA or other regional bodies contribute?

What role can regional bodies such as the APPA Forum, or even the Asian regional office of UNESCO (based in Seoul) play in these complex developments in the Asia-Pacific? It is clear that there is no one way forward for the development of privacy standards in the Asia-Pacific. The APEC processes are not and should not be the only international forums for the debate and development of privacy laws, particularly given how they are dominated by government and business interests. However, the APEC processes can constructively coexist and cooperate with other forums.

One of the most constructive things that other regional bodies can do is to provide or co-host regional privacy forums that assist to legitimate and make known alternative approaches to dealing with regional and national privacy issues. In particular, APPA can make the voice of privacy Commissioners heard, and UNESCO can help give a voice to civil society organisations.

The Montreux Declaration calls for the development of a UN privacy treaty, and at the same time invites examination of the Council of Europe privacy Convention as an interim vehicle for global privacy standards. These issues need to be debated at the Asia-Pacific level (now that we have finished debating a regional agreement for the time being). Who will play a leading role in facilitating that debate depends to a large extent on who is willing.

References

('PLPR' is *Privacy Law and Policy Reporter*, available at <http://www.austlii.edu.au/au/journals/PLPR/>)

Abrams (2005) - Martin Abrams, Executive Director, Center for Information Policy Leadership, Hunton & Williams 'Educating and Publicizing Domestic Privacy Protection' (at HK Seminar (2005))

Bendrath (2005) – Ralph Bendrath 'UN WSIS and privacy', paper presented at University of Edinburgh, September 2005

APC (2005) – Australian Privacy Commissioner *Review of the private sector provisions of the Privacy Act*, 2005, available at <http://www.privacy.gov.au/act/review/index.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 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>.

APPCC (2003) - Asia-Pacific Privacy Charter Council website <http://www.bakercyberlawcentre.org/appcc/>

APT (2003) - Asia-Pacific Telecommunity's Privacy Guidelines (The APT website is <http://www.aptsec.org/index.html> but the Guidelines do not seem to have been made public. A copy is on file with the author.)

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

A29 Committee Tasks – 'Tasks of the Article 29 Data Protection Working Party' http://europe.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/tasks-art-29_en.pdf

BNA (2006) – *BNA Privacy Law Watch*, 23 February 2006, quoting the US Council for International Business, US government representatives and others.

Changbeom (2005) - Dr. Yi Changbeom, Acting Vice President, Korea Information Security Agency (KISA), Personal Information and Privacy Protection Division 'Remedy for Personal Information Infringement in Korea' (at HK Seminar (2005))

Bygrave (1998) - Lee Bygrave Data Protection Pursuant to the Right to Privacy in Human Rights Treaties (1998) 6 Int J of Law and Information Technology, no 3, 247-284

Clarke (2000) - Roger Clarke 'Beyond the OECD Guidelines: Privacy Protection for the 21st Century' (2000) <http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html>

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>

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)

Data Protection Working Party (2001) - Data Protection Working Party *Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000*, available at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2001/wp40en.pdf

EPIC, 2003 – *Electronic Privacy Information Centre Privacy and Human Rights – An international survey of privacy laws and developments*, EPIC, Washington, 2003

European Union (1995) - Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data*

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

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

Greenleaf (2005c) – Graham Greenleaf '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 (forthcoming, 2005)

Greenleaf (2005b) - Graham Greenleaf, University of New South Wales, Convener of the Asia-Pacific Privacy Charter Council, Australia 'Appropriate Remedies for APEC's Privacy Framework' (at HK Seminar (2005))

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

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

Greenleaf (2004) - Graham Greenleaf '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) - Graham Greenleaf 'APEC Privacy Principles Version 2 - Not quite so Lite, and NZ wants OECD full strength' (2003) 10(3) PLPR 45

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

Greenleaf (2000) - Graham Greenleaf 'Private Sector Bill amendments ignore EU problems' (2000) 7 PLPR 41

Greenleaf (2000a) - Graham Greenleaf 'Safe Harbor's low benchmark for 'adequacy': EU sells out privacy for US$' [2000] PLPR 32

Greenleaf (1999) – Graham Greenleaf 'Transborder data flow controls - regional perspectives and examples' *Proc. Second Asia Pacific Forum on Privacy and Data Protection*, 1999, Hong Kong

Greenleaf (1998) - Graham Greenleaf 'Global Protection of Privacy in Cyberspace - Implications for the Asia-Pacific' particularly Part 6. 'Towards an Asia-Pacific information privacy Convention?' *1998 Internet Law Symposium* <http://austlii.edu.au/itlaw/articles/TaiwanSTLC.html>, Science & Technology Law Center, Taipei, Taiwan, 23-24 June 1998

Greenleaf (1996) - Graham Greenleaf 'Stopping surveillance: beyond `efficiency' and the OECD' (1996) 3 PLPR 148

Greenleaf (1995) – Graham Greenleaf 'Towards an Asia-Pacific information privacy convention' (1995) 2 PLPR 127-131

Heyder (2005) - Markus Heyder, Legal Advisor, Bureau of Consumer Protection, U.S. Federal Trade Commission 'Remedies for Privacy Violations' (at HK Seminar (2005))

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.>

Hughes (2001) - Aneurin Hughes 'A Question of Adequacy? The European Union's Approach to Assessing the Privacy Amendment (Private Sector) Act 2000 (Cth)' [2001] UNSWLJ 5, available at http://www.austlii.edu.au/au/journals/UNSWLJ/2001/5.html

iPP website - <http://www.cyberlawcentre.org/ipp>

Rikke Frank Jørgensen 'A Human Rights Perspective on the Word Summit on the Information Society. The Human Rights Framework' in Heinrich Böll Foundation (ed.), Visions in Process, World Summit on the Information Society, Geneva 2003 – Tunis 2005 available at <http://www.worldsummit2003.de/download_de/Vision_in_process.pdf >

Kirby (2003) - 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 200

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

Rainer Kuhlen ' The Charter of Civil Rights for a Sustainable Knowledge Society – A Vision with Practical Consequences' in Heinrich Böll Foundation (ed.), Visions in Process, World Summit on the Information Society, Geneva 2003 – Tunis 2005 available at <http://www.worldsummit2003.de/download_de/Vision_in_process.pdf >

Lam (2005) – Tony Lam, Acting Privacy Commissioner for Personal Data, Hong Kong 'An Overview of the Principles Established by the APEC Privacy Framework' (at HK Seminar (2005))

Mandy Rice Davies (1963) – see <http://en.wikipedia.org/wiki/Mandy_Rice-Davies>

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

OECD (1981) - OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, 1981

Rotenberg (1988) - Marc Rotenberg Preserving 'Privacy In The Information Society' UNESCO InfoEthics Forum, 1998 <www.**unesco**.org/webworld/infoethics_2/eng/papers/paper_10.htm>

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))

Stewart (2006) - Blair Stewart 'Privacy Commissioners adopt ambitious regional objectives' (2006) 11(8) PLPR 221

Waters (2000) - Nigel Waters 'Rethinking information privacy — a third way in data protection? ' (2000) 6 PLPR 121

WSIS (2005) – WSIS website <http://www.wsis.org>

WSIS Declaration (2003) – WSIS *Declaration of Principles - Building the Information Society: a global challenge in the new Millennium*, Geneva 2003 <http://www.itu.int/wsis/docs/geneva/official/dop.html>

WSIS Tunis Commitment (2005) http://www.itu.int/wsis/docs2/tunis/off/7.html

Appendix: Asia Pacific Privacy Authorities Forum - Statement of Objectives

Meeting in Melbourne, Australia, on 17 November 2005, the assembled privacy authorities from Australia, Hong Kong, Korea and New Zealand, resolved as follows:

RECOGNISING that:

- Privacy is a matter of growing international concern
- Information networks closely connect people and organisations in our various jurisdictions regardless of physical borders and differing laws
- Governments and business expect regulators to strive for efficient and effective solutions and that best practice requires privacy authorities to be aware of what similar regulators are doing
- Privacy issues can emerge in one jurisdiction before others and that privacy authorities can benefit from an advanced warning system
- Privacy authorities are increasingly being called upon to contribute to solutions to complaints, or policy challenges, that cross borders
- There is limited specialised data privacy resource in any one jurisdiction and that privacy authorities benefit from reaching abroad for information, inspiration and assistance
- Participants in the forum will benefit from cooperation in information privacy knowledge sharing and technical resources
- Adoption of the APEC Privacy Framework in 2004 has provided a regional restatement of the importance of privacy and transborder information flows and a spur to reinvigorate regional cooperative arrangements

THEREFORE we resolve to:

- Continue the cooperative arrangements established in 1992 and which came to be known as PANZA+ in the ensuing 24 meetings
- Rename the meeting as the Asia Pacific Privacy Authorities Forum
- Encourage further participation from within the region

AND FURTHER RESOLVE to build upon and enhance the current arrangements with the principal objectives of:

- Facilitating the sharing of knowledge and resources between privacy authorities within the region
- Fostering cooperation in privacy and data protection
- Promoting best practice amongst privacy authorities
- Working to continuously improve our performance to achieve the important objectives set out in our respective privacy laws.

Privacy Commissioner of Australia
Privacy Commissioner of New Zealand
Privacy Commissioner for Personal Data, Hong Kong SAR
Privacy Commissioner of New South Wales, Australia
Privacy Commissioner of Victoria, Australia
Information Commissioner of Northern Territory, Australia
Korea Information Security Agency