The APEC Privacy Framework

Creating Trust in developing Cross-Border Privacy Rules: A Progress Report

Malcolm Crompton

Managing Director
Information Integrity Solutions

March 2007

The APEC Privacy Framework

Creating Trust in developing Cross-Border Privacy Rules: A Progress Report

Introduction

Nowhere else in the world is the handling of personal information increasing and transforming more rapidly than around the Pacific Rim, with the possible exception of India.

The region's pre-eminent economic grouping, APEC, has recognised a key to economic growth through eCommerce is the free flow of personal information in a way that respects privacy. It has become very clear that the barrier to achieving this goal is the emerging problem of cross border data flows where information collected in one economy is processed in another. In the context of privacy regulation, the challenge is made more difficult because privacy and data protection regulation is usually bound to a local jurisdiction and can only 'see' and regulate the information flows in that jurisdiction. On the other hand, data processing is increasingly global.

Business has played a leading role in these developments and has a very significant stake in the successful implementation of a practical and effective region wide privacy framework.

This paper describes the very rapid progress being made by APEC in addressing the issues and finding solutions that seek to address 21st Century realities in a very diverse region.

The 2007 and 2008 APEC work program on privacy

The APEC Privacy Framework was adopted by APEC Ministers in 2004. In their 2006 Annual Statement, Ministers emphasised the need to ensure "responsible and accountable Cross-Border information flows and effective privacy protection without creating unnecessary barriers". They acknowledged the role that the cross border rules concept could play in achieving this goal. Ministers also "encouraged Officials to facilitate this goal by developing and disseminating implementation frameworks such as best practices for Cross-Border rules".[1] More detailed background information about APEC and the development of the APEC Privacy Framework are set out at Appendix A.

As the host of APEC 2007 meetings Australia has acted on this guidance. It successfully applied for funding to host two two-day technical seminars on the international implementation of the APEC Privacy Framework. The seminars are intended to provide a forum for business, government and consumer groups to discuss the implementation of Cross-Border Privacy Rules and to develop options for a pathfinder options to be pursued in 2008. They are also intended to inform the more formal processes of APEC through reports to the Data Privacy Subgroup of APEC's Electronic Commerce Steering Group (ECSG).

[1] **Cross-border privacy rules** (CBPRs) are a set of rules developed by an organisation which it commits to apply to its activities involving transfers of personal information across borders. With the wide range of approaches to privacy frameworks applying to personal information across APEC economies, APEC has decided that facilitating the use of, compliance with and enforcement of CBPRs was a particularly good place to start for implementing the APEC Privacy Framework as it applies to personal information when it moves across borders.

Data Privacy Subgroup Seminar on Cross-Border Privacy Rule (CBPRs), Canberra, Australia 22-23 January 2007

The first technical seminar was held in Canberra, Australia on 22 and 23 January 2007. Some 16 economies were represented by over 100 delegates. The seminars were organised by the Attorney-General's Department of the Australian Government. Malcolm Crompton of Information Integrity Solutions was retained to provide advice and assistance in developing the program, engaging speakers and writing discussion papers.

The objective of the first seminar was creating trust in developing Cross-Border privacy rules: making compliance possible and enforcement credible when personal information moves between economies.

The seminar began by providing a forum for government, business and consumer groups to give their perspective on the problem of how to keep the original privacy promise made when information is collected in one economy but then processed in another. All speakers made the point early on that a win-win result is possible, ie more effective protection of personal information can be provided to individuals and be achieved by putting in place regulatory frameworks that businesses can comply with more efficiently. First signs of the new framework are already emerging, including cooperation between regulators over cross border privacy regulation. The Australian and New Zealand privacy regulators signed Memoranda of Understanding (MOU) based in part on the APEC Framework in September 2006.[2] The Asian Trustmark Alliance is also seeking to respond to the challenges thrown out by the APEC Privacy Framework.

On the second day the seminar focused on three implementation models developed in a Discussion Models Paper. A summary of the discussion models from this paper are included here as Appendix B.[3]

Three breakout groups considered the options in detail. The seminar concluded with sessions that summarised these discussions in order to provide useful input to the Data Privacy Subgroup's consideration of the challenges faced in developing a pathfinder project and moving towards implementation of CBPRs.

The approach to considering the implementation models focused on starting with a small number of APEC economies developing an efficient, enforceable compliance and complaints handling framework that is workable in the APEC region which contains a diverse range of data protection regimes. Consistent with the pathfinder concepts in APEC, the scope of the implementation models were limited to covering organisations that volunteer to opt in to be covered by cross border privacy rules in economies that volunteered to implement the rules. It was envisaged that the scheme would expand later if successful.

Successful Cross-Border privacy protection: what does success look like?

While there is widespread agreement that the privacy protection of personal information must be ensured, there is more work to be done on defining a successful protection framework. To

---

[2] See of the announcement by the Privacy Commissioner of Australia on 19 September 2006, available online at: www.privacy.gov.au/news/06_20.html

[3] The key papers for considering the model implementation options during the seminar were:
Cross-Border Privacy Rules Implementation Discussion Paper
(APEC paper number 2007/SOM1/ECSG/SEM002), and
Discussion Models for Breakout Session
(APEC paper number 2007/SOM1/ECSG/SEM003)
All seminar papers will be available online at:
www.apec.org/apec/documents_reports/electronic_commerce_steering_group.html

this end, the Discussion Paper suggested specific success criteria for the models that the seminar evaluated.

The first criteria suggested in the Discussion Paper came direct from the APEC Privacy Framework. In particular, drawing on paragraph 48 of the Framework, the following success criteria were formulated:

- Does the model facilitate responsible and accountable Cross-Border data transfer?
- Does the model facilitate effective privacy protections?
- Does the model avoid creating unnecessary barriers to information flows and unnecessary administrative and bureaucratic burdens?

Other success criteria included:

- Does the model ensure that privacy promises made at the local level are met as data is processed globally?
- Does the model provide credibility to the main stakeholders (ie. consumers and business)?

Importantly, where the seminar identified impediments in current legal frameworks to an otherwise preferred model, participants were asked to find ways of minimising such impediments and spell out clearly what might be needed to remove those that remain. Hence additional success criteria for each model were:

- Can the model be implemented within the current domestic legal frameworks of the participating APEC economies and within current international legal frameworks?
- If there are legal impediments, have these been minimised?
- Are any outstanding legal impediments clearly identified so that economies participating in a pilot or pathfinder can consider whether and how they might address them?

The emphasis of the seminar was that the CBPR system being considered at this point was not seeking to improve domestic privacy protections within participating APEC economies.

In order to facilitate their work, the breakout groups were provided with a Discussion Models Score Card for use during discussion and for reporting back to the seminar plenary sessions. The Score Card is included here as Appendix C.

Testing the Discussion Models

On Day 2 of the seminar each participant had the opportunity to participate in break out group discussion on 2 of the 3 models in the Discussion Models.

Discussion Group leaders reported back with a general view that Model 1, the "Choice of Approach" was the most promising, supported by elements of the Model 3 "APEC Region Trustmark". The more that Trustmarks could take care of the basics such as broad advice to business on good practice, cover compliance processes, provide advice to consumers and handle complaints, the more that government regulators and law enforcement could focus on the most harmful and malevolent end of the spectrum.

Model 2 "Council of Regulators" was seen as least promising.

Any model was seen to need the support of:

- Significant documentation, eg Standards expected in order for one economy to be able to trust the arrangements made by another including any Trustmark arrangements put in place; Instructions, Self Assessment templates for applicant businesses etc;
- A possible 'model rule' to provide a starting place for businesses to consider when drawing up their CBPR
- 'Shopfront' processes for both consumers and businesses such as a single website that lists all businesses with complying CBPRs, provides a single point of contact for advice on and lodging consumer complaints and provides links to all advice and documentation for businesses
- Education for consumers, business, government

Conclusion of the Seminars – The purpose of any Cross-Border privacy framework is Creating Trust

In summing up, David Loukidelis, Privacy Commissioner for British Columbia emphasised the importance of making a start. New insights into effective regulation included the importance of picking a fixable problem and fixing it and in this way beginning a process of confidence building. In any pathfinder, a clear description of the problem being solved needs to be spelt out. He also summarised by saying that any implementation for pursuit as a pathfinder needs to be:

- Flexible but Certain
- Efficient but Effective
- Trusted by all – governments, business, consumer and regulator
- Consistent with domestic regimes

It was noted several times during the seminar that, consistent with Principle 9 in the APEC Privacy Framework, a key desired outcome of any future implementation of an expanded CBPR system (ie. following successful outcomes from initial pathfinder processes) would ideally be as follows: a system that ensures that initial privacy protections (comprising the law applicable at the time of the data collection, the organisation's privacy policy at the time of collection and any choices made by the consumer at the time of collection) are observed and enforced regardless of how many of the participating APEC economies are involved in the subsequent handling of the personal information.

Outcome of Data Privacy Subgroup and ECSG Meetings, Canberra Australia 24-25 January 2007

The Data Privacy Subgroup met immediately after the seminar followed by a regular meeting of ECSG. Both meetings considered the consultants report of the seminar and the application of CBPRs across a broad range of situations including under existing privacy law.

The meeting supported the proposal that frameworks for accountable cross border transfers of personal information had to be flexible, credible and enforceable to be implemented in a range of economies.

The most significant outcome of the meetings was support for a Pathfinder Proposal framework that set out key objectives that would form the basis of particular projects to be

implemented as part of putting together a CBPR compliance system across economies. The proposed Pathfinder's main objectives in the promotion of accountable cross border information flows are:

1. **Conceptual Framework Principles**. Promoting a conceptual framework of principles of how cross border rules should work across economies, and the various parties that may be actors in the implementation and enforcement of these rules.

2. **Consultative Process**. Promoting the development of consultative processes on how to best include stakeholders including regulators, responsible agencies, lawmaking bodies, Industry, third party privacy providers and consumer representatives both in the creation of the rules and processes and in their operational review and optimization.

3. **Practical Documents.** Promoting the development of the practical documents and procedures that underpin cross border rules such as self-assessment forms, review criteria, recognition/acceptance procedures and dispute resolution mechanisms.

4. **Implementation.** Exploring ways in which various documents and procedures may be implemented in practices with due consideration to the mandates of the parties involved and the legal frameworks in which they operate, and

5. **Education and Outreach.** Promoting education and outreach that will be needed to allow stakeholders and potential participants to consider how to enable accountable data flows across the participating economies.

It was agreed that the Pathfinder project framework paper would be developed and prepared for discussion through the Economic Commerce Steering Group. It was noted in the meeting that the Pathfinder project requires the support of 50% of APEC economies. At this stage Australia; Canada; Hong Kong, China; Mexico; Singapore; Chinese Taipei; United States stated that they may be able to support such a Pathfinder project. All economies were urged to consult domestically and consider whether they could support the Pathfinder framework in the coming months. It was noted by the Chair that support for this Pathfinder framework was not support for a single project, but a framework for implementing specific projects that the economies may choose to be involved in.

In terms of developing specific projects, a number of initiatives are already under way:

- Canada has agreed to lead a group of regulators to further discuss Cross-Border enforcement cooperation among privacy and consumer protection regulators.
- Mexico has indicated it would seek to host a Trustmark forum in early May.
- The Asian Trustmark Alliance will use its forthcoming conference to focus on how the Alliance can contribute to the development of the CBPR compliance framework.

Next Steps – the Second Technical Seminar, Cairns, 22-23 June 2007

Planning is now under way for the second of the technical assistance seminars. The second seminar will be held in Cairns in Queensland, Australia on 22-23 June 2007 and will be followed by meetings of the Data Privacy Subgroup then the ECSG. The aim will be to have agreement on establishing a Pathfinder framework and concrete agreement on Pathfinder projects. In order to achieve this, framework documentation along the lines identified by the breakout Discussion Groups will have to be largely drafted by the time of the Cairns seminar.

APPENDIX A

Background to the APEC Privacy Framework

What is APEC?

The Asia-Pacific Economic Cooperation forum, or APEC, is an international group of economies that work to facilitate economic growth, cooperation, trade and investment in the Asia-Pacific region.

APEC operates on the basis of non-binding commitments, open dialogue and equal respect for the views of all participants. 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. This means that when economies wish to do so, they can move very rapidly to address issues of concern.

APEC has 21 members – referred to as "Member Economies" – which account for approximately 40% of the world's population, approximately 56% of world GDP and about 48% of world trade. This includes the largest economy in the world, the United States of America and the economy with the world's largest population, China.

APEC's 21 Member Economies are Australia; Brunei Darussalam; Canada; Chile; People's Republic of China; Hong Kong, China; Indonesia; Japan; Republic of Korea; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; The Republic of the Philippines; The Russian Federation; Singapore; Chinese Taipei; Thailand; United States of America; Viet Nam.

Why does it matter? The APEC Privacy Framework

In November 2004 APEC Ministers endorsed the APEC Privacy Framework.[4] The Framework took only 2 years to develop, a remarkable achievement in any international forum. The work was undertaken by the Data Privacy Subgroup of APEC's Electronic Commerce Steering Group (ECSG).

The APEC Privacy Framework correlates closely with the Organisation for Economic Cooperation and Development's (OECD) 1980 Privacy Guidelines. It outlines nine privacy principles which cover preventing harm, notice, collection limitation, uses of personal information, choice, integrity of personal information, security safeguards, access and correction and accountability.

The APEC Privacy Framework was developed to assist APEC economies introduce domestic privacy law and to address the privacy protection of personal information when it moves between economies. The framework includes new insights not seen so clearly in earlier frameworks. These are:

- Principle 1, which emphasises the importance of focusing first on where harm is greatest; and
- Principle 9, which in essence states that accountability remains with the original personal information controller, even if the information is passed on to others.

[4] The APEC Privacy Framework can be downloaded from www.apec.org/apec/apec_groups/som_special_task_groups/electronic_commerce.html.

In full, Principle 9 states that:

> *"A personal information controller should be accountable for complying with measures that give effect to the [APEC Information Privacy Principles]. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles".*

The current position

Cross-border privacy rules (CBPRs) are a set of rules developed by an organisation which it commits to apply to its activities involving transfers of personal information across borders. With the wide range of approaches to privacy frameworks applying to personal information across APEC economies, APEC has decided that facilitating the use of, compliance with and enforcement of CBPRs was a particularly good place to start for implementing the APEC Privacy Framework as it applies to personal information when it moves across borders.

Indeed, in their 2006 Annual Statement, Ministers emphasised the need to ensure "responsible and accountable Cross-Border information flows and effective privacy protection without creating unnecessary barriers". They acknowledged the role that the cross border rules concept could play in achieving this goal. Ministers also "encouraged Officials to facilitate this goal by developing and disseminating implementation frameworks such as best practices for Cross-Border rules".

Hence the Data Privacy Subgroup work agenda for 2007 is focused on developing options for pathfinder projects that would be pursued in 2008 for giving effect to binding CBPRs. It has chosen CBPRs as a particularly good place to start for implementing the APEC Privacy Framework as it applies to personal information when it moves between economies. This is because CBPRs may be a simpler and more tractable subset of the challenges of putting in place privacy protection for personal information when it moves between economies and the strong interest by some businesses in putting in place a framework to support such rules.

The intention is that any options adopted as a pathfinder project in 2008 would be evaluated at the end of the pathfinder period. If one or more were considered to have worked well, they could become the basis for expansion into a wider implementation framework for APEC and the involvement of more APEC economies.

APPENDIX B

Model 1 – 'Choice of Approach' Model

Summary of Model

The key feature of this model is that each economy chooses the entities and procedures that will be used within the economy to assess the compliance of an organisation's Cross-Border privacy rules (CBPRs) with the APEC Privacy Framework.

An organisation that wishes to be considered as having CBPRs that comply with the APEC Privacy Framework submits an application containing its self-assessment (for example, this could be a standard form questionnaire developed by the participating economies) to the designated review entity in the participating economy relevant to the organisation (eg. the economy where the organisation's head office is located).

By a framework agreed between the relevant entities of the participating economies (eg. through a series of Memoranda of Understanding or official letters of commitment), a process is established to publish a centralised publicly available list (eg. on a single website) of the names of organisations whose CBPRs are assessed by designated review entities as being compliant with the APEC Privacy Framework.

Under the agreed framework, a participating economy accepts the assessments made by the designated entity in another participating economy following the choice of approach to CBPRs in that economy (eg. one economy may have a privacy commissioner it designates to make assessments and another economy may choose to use existing Trustmark bodies, but it would be agreed that a decision by either entity to include an organisation on the list would be accepted).

The agreed framework also provides for communication and information sharing between the designated entities in each economy to facilitate the resolution of disputes relating to consumer complaints on Cross-Border handling of personal information.

Key aspects

(a) **Designated review entity in each economy** – each participating economy would designate an entity (or entities) of its choice for receiving and reviewing applications for assessment of the compliance of an organisation's CBPRs against the APEC Privacy Framework, publishing details of compliant organisations, monitoring ongoing compliance, and handling complaints.

(b) **Forum of designated entities** – participating economies would establish a forum of each of the designated entities from all the participating economies. This forum could set minimum standards for compliance assessment, prepare template documents for use as part of the assessment process, or develop guidance for organisations and consumers about the system.

(c) **List of compliant organisations –** a centralised list accessible to the public that contains the details of organisations in all participating economies that have been found by the designated entity in the participating economies to have CBPRs that satisfy the requirements of the APEC Privacy Framework.

(d) **Coordination of complaint handling** – participating economies would establish a framework for handling complaints regarding Cross-Border handling of personal information. This could be an APEC-wide online 'shopfront' where consumers can lodge complaints which are then distributed to the relevant economies for investigation and further appropriate action.

Model 2 – Council of Regulators Model

Summary of Model

This model establishes as its central body a council consisting of 'regulators' from each participating APEC economy (Council). A 'regulator' would be a government-established regulatory entity or supervisory authority in the participating economy (eg. a privacy commissioner or consumer protection authority established by legislation but independent of government).

Each participating economy designates a regulator as its representative on the Council. The legal basis for the participation of each economy's regulator in the Council is the domestic law of that economy (which may require amendment to enable the regulator's participation), but the Council itself is established by way of interlocking Memoranda of Understanding (MOUs) between participating economies.

An organisation that wishes to be considered as having Cross-Border privacy rules (CBPRs) that comply with the APEC Privacy Framework applies to the Council for assessment of its CBPRs. The Council arranges for the review and assessment of the CBPRs submitted by organisations in accordance with a Council agreed process (eg. the Council could refer the application to the regulator in the economy in which the organisation has its global headquarters to make an assessment on behalf of all regulators, or distribute the application to all the regulators for their combined input into an assessment).

Organisations that are assessed through the Council process as having CBPRs that comply with the APEC Privacy Framework are provided with some form of approval, such as an advisory statement, branding, listing on a website or other mechanism for representing their compliance to the public.

The Council coordinates the taking in of consumer complaints regarding Cross-Border handling of personal information and refers complaints to the appropriate designated regulator (eg. the regulator from the complainant's home economy, or the economy in which the responding organisation is based). The Council establishes a process for individual regulators to respond to such complaints, share information with other regulators relevant to the complaint, and take enforcement action.

Key aspects

(a) **Designated 'regulator' from each participating economy** – each participating economy would designate a government-established regulatory entity or supervisory authority (eg. a privacy commissioner or consumer protection authority) as its representative on the council of regulators and to perform a role as part of the CBPR system established through the Council.

(b) **Council of regulators** – participating economies would establish a council of their designated regulators, to coordinate the actions of individual regulators in each participating economy. The Council would have functions such as coordinating the assessment of organisations' CBPRs against the APEC Privacy Framework, setting standards for such assessments, issuing a form of approval to compliant organisations and assisting to resolve consumer complaints regarding Cross-Border personal information handling. The Council would be established through a framework of MOUs between the participating economies.

(c) **Council coordination of complaint handling** – the Council would agree on procedures for taking in and distributing consumer complaints to the appropriate regulator for investigation, and the actions to be taken by different regulators where a complaint related to the jurisdictions of multiple regulators.

Model 3 – APEC Region Trustmark Model

Summary of Model

This model establishes a Cross-Border privacy rules (CBPR) system based on a group of Trustmark programmes in the participating APEC economies being linked by a harmonised set of rules and supported by enforcement cooperation among relevant authorities in those participating economies. In this paper, the system will be referred to as the 'APEC Online Trustmark System (APECOTS)'.

Each participating economy designates a Trustmark entity as an 'APECOTS Operator' to coordinate in that economy the issuing of the APECOTS Trustmark to organisations that have applied and had their CBPRs assessed as compliant with the APEC Privacy Framework. The APECOTS Trustmark shows consumers that the organisation has been assessed as having met the APECOTS standards for Cross-Border handling of personal information. APECOTS Operators can be existing Trustmark entities (whether private, public or semi-public) in the participating economies, providing the opportunity for co-branding the 'local' Trustmark with the APECOTS Trustmark.

APECOTS is self-regulatory to the extent that an organisation can sign up to the system voluntarily. However, for the time an organisation participates in the CBPR system, it is legally bound to comply with system rules, including decisions of the oversight bodies for APECOTS. Each participating economy has a government enforcement authority that is able to support APECOTS and investigate, make and enforce decisions regarding CBPR related complaints, to provide a further safety net for the operation of the system.

APECOTS is coordinated across the APEC region through a network of the APECOTS Operators, and an oversight body for APECOTS consisting of government designated representative bodies from each participating economy.

Key aspects

(a) **Trustmark entity in each participating economy** – each participating economy designates a Trustmark entity to be the operator of the system in that economy (APECOTS Operator).

(b) **Network of APECOTS Operators** – a network of APECOTS Operators from each participating economy would be established to set minimum standards for compliance assessment, prepare template documents for use as part of the assessment process, or develop guidance for organisations and consumers about the system.

(c) **Government enforcement authority in each participating economy** – each participating economy will have a government enforcement authority (eg. a privacy commissioner or consumer protection authority) with statutory powers that enable it to enforce the APEC Privacy Framework in some way (eg. by enforcing decisions of the economy's APECOTS Operator in response to consumer complaints, or receiving complaint referrals from the APECOTS Operator which it can investigate independently, make a decision on and enforce). These enforcement authorities may need to form a cooperative network for handling CBPR related complaints involving more than one economy.

(d) **APECOTS oversight body for coordinating the system** – an oversight body consisting of government designated representative bodies from each participating economy would be established to oversee the system (eg. approve the APECOTS code of practice).

APPENDIX C

Discussion Models Score Card

Question	Yes	No	Impediments to Implementation	Impediments to Trust
Self-Assessment				
Will this model facilitate guidance to business on how to self-assess their policies and procedures to assure they reflect APEC Information Privacy Principles?				
Will this model facilitate consistency in the instructions given to businesses in the interim pathfinder economies?				
Will this model facilitate consumer understanding of the self-assessment process?				
Compliance Review				
Does this model facilitate the designation of recognized parties within economies to review assertions?				
Does this model facilitate mechanisms to assure these review parties have the required skills and authority?				
Does this model facilitate oversight over review parties?				

Question	Yes	No	Impediments to Implementation	Impediments to Trust
Recognition/Acceptance				
Does this model facilitate communication of an approved CBPR to other economies?				
Does this model facilitate knowledge by interested parties of the identity of the approving party?				
Does this model facilitate trust in quality of work undertaken by the approving party in reviewing the CBPR?				
Dispute Resolution/Enforcement				
Does the model facilitate consumer knowledge of how to use dispute resolution process?				
Does the model facilitate knowledge by businesses with CBPRs on how the cross-border dispute process will work?				
Does the model facilitate the ability for the accountability agent in one economy to hand off investigation to the appropriate agent in another economy?				
Does the model facilitate keeping a dispute between a consumer and a CBPR holder within a local jurisdiction?				

Question	Yes	No	Impediments to Implementation	Impediments to Trust
Flexibility				
Does this model make allowances for the differences in privacy laws and enforcement procedures that exist in the APEC region?				
Trust				
Does this model facilitate consumer trust that they will be protected when data moves across borders?				
Does this model facilitate trust by business that the approval and enforcement processes will be predictable?				
Does this model build trust by governments that their citizens and businesses will be treated fairly?				