



Asia-Pacific  
Economic Cooperation

---

**2006/SOM1/ECSG/SYM/002**

Agenda Item: 1

## **APEC Information Privacy Framework (review, impact, and progress)**

Purpose: Information  
Submitted by: Australia



**APEC Symposium on Information  
Privacy Protection in E-Government  
and E-Commerce  
Ha Noi, Viet Nam  
20-22 February 2006**



INFORMATION  
INTEGRITY  
SOLUTIONS

# Malcolm Crompton

## *APEC Information Privacy Framework: review, impact, & progress*

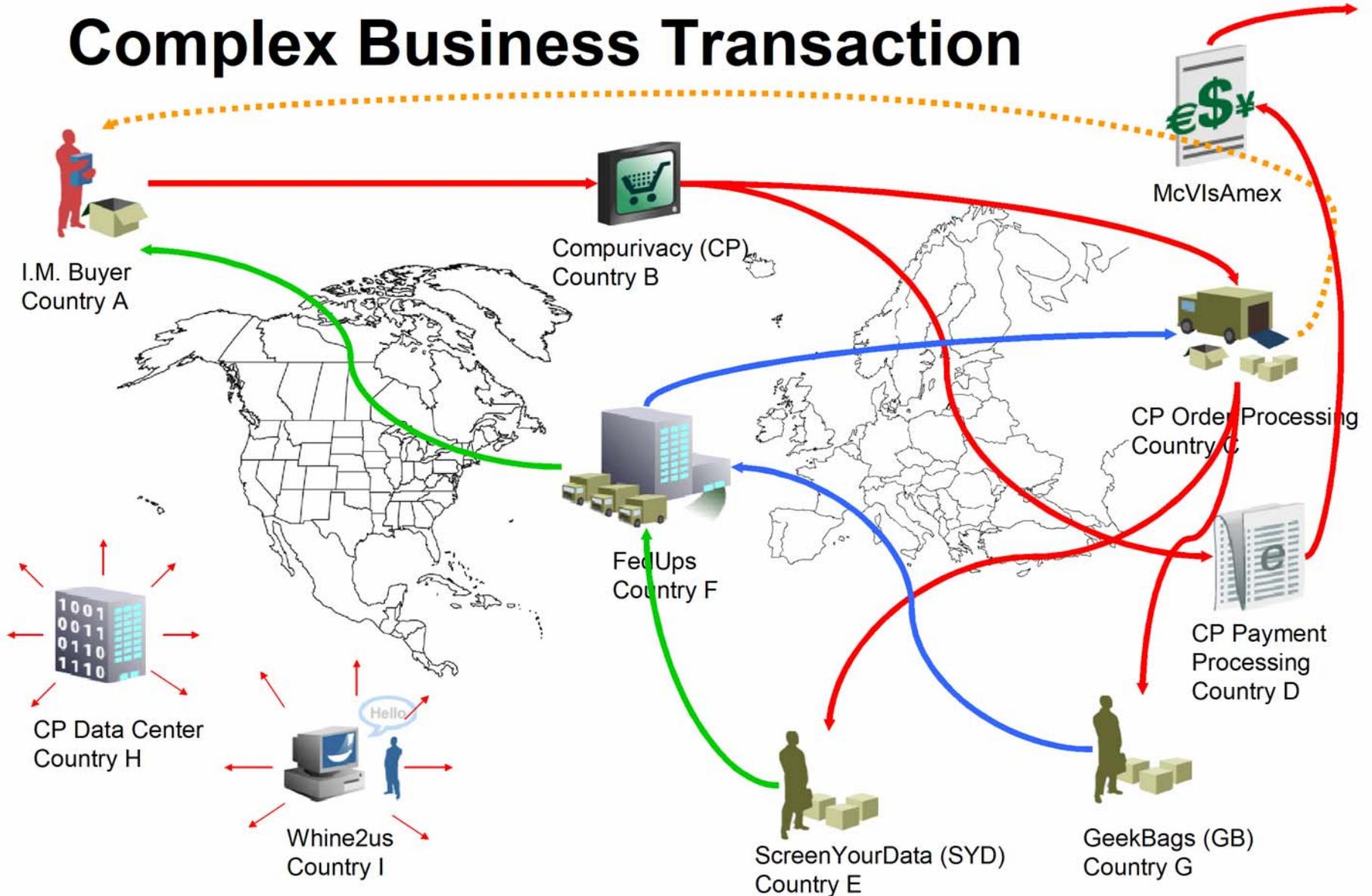
APEC Symposium on Information Privacy  
Protection in E Government & E Commerce

*Hanoi  
20 February 2006*



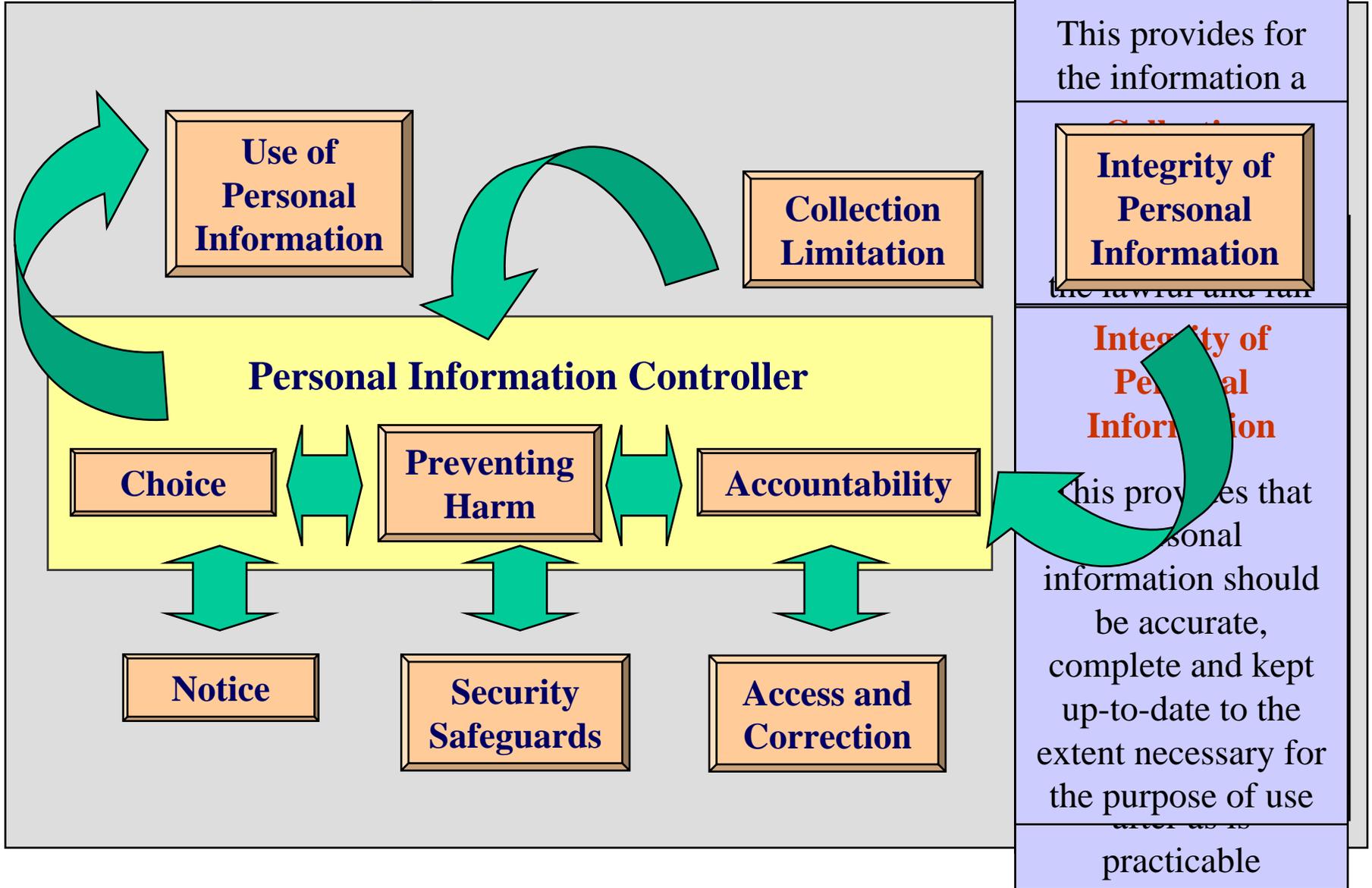
Why is 'Privacy' on the  
APEC agenda?

# Complex Business Transaction



# The APEC Privacy Framework

# APEC Privacy Principles: Relationship



# Nine APEC privacy principles

1. Preventing Harm – privacy protections should focus on preventing harm and misuse
2. Notice – clear & easily accessible
3. Collection Limitation – collect what's relevant in a lawful & fair manner
4. Uses of Personal Information – for expected and compatible purposes, with consent, or where necessary
5. Choice – where appropriate, provide clear, accessible mechanism to exercise choice

## Nine APEC privacy principles

6. Integrity – personal information should appropriately accurate, complete and up-to-date
7. Security – appropriate safeguards to protect against unauthorized access, use, modification or disclosure
8. Access & Correction – important (but not absolute) rights
9. Accountability – controllers are accountable for compliance with all Principles and must use reasonable steps to ensure that recipients of personal information also comply

# The APEC Insight

# Insight in Principles 1 & 9

## Principle 1

- Proportionality: focus effort on where harm greatest

## Principle 9

- ‘Accountability follows the data’



Where did we get to last  
time?

## What is the problem?

- Complex business transactions makes privacy compliance more difficult
- Many laws, many regulators
  - Hard for anybody to see the whole
- Effective resolution of complaints
  - Cost to business; cost to consumer
- Justification introducing privacy regime for a small economy not a small task
  - International trade argument very strong

## Immediate action

- Consumer empowerment
  - Improved Privacy Notices
- Education – effort from Govt; business; hot topics like ID theft
  - Consumers
  - Business, especially small business
- Privacy Regulators encouraged to coordinate more
- Business to pay more attention to flows of personal information in their business and with their business partners
- But turn this into a strategy – How?

# Implementation

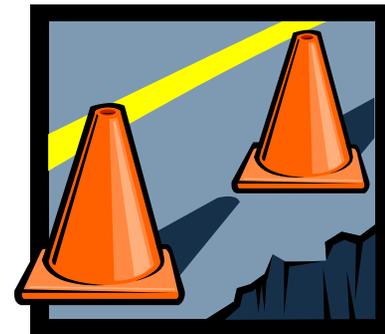
# Governance

‘Safety begins at home’

- those directly handling the data to respect and abide by that framework

Internal Privacy Governance Framework

- A high level policy
- Standard operating procedures
- Recommended measures & best practices
- Training ,communication & compliance tools
- Assurance functions



# Domestic

- 6 APEC Member Economies have broad based privacy law
- 1 has sectoral law
- 1 has voluntary framework
- At least 5 drafting a privacy framework

Consistency with APEC Privacy Framework varies

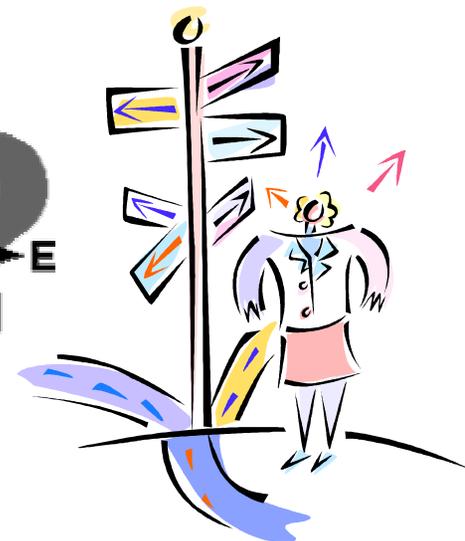
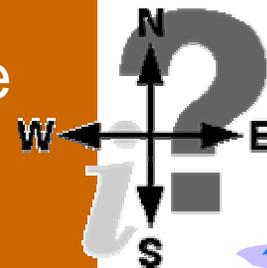
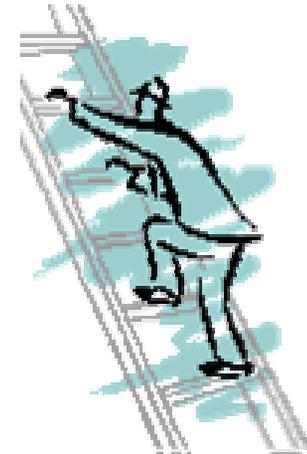


# International

APEC Member Economies have most to do here

## Options

- ‘APEC Privacy Commission’
- NGO equivalent, either one or more
- Binding corporate rules
- Cooperative arrangements between existing privacy regulators



# International

## Part B:

- “44. Member Economies should ... facilitate cross-border cooperation in the enforcement of privacy laws
- “46. Member Economies will endeavor to support the development and recognition or acceptance of organizations’ cross-border privacy rules across the APEC region ... that ... adhere to the APEC Privacy Principles.”



# Further work

Build on 2005

- See consultants' Final Report

Facilitate Binding Corporate Rules

- a. Industry accountability checklist
- b. Process for “approvals” of rules
- c. International trust on enforcement

Information Privacy Individual Action Plans

OECD privacy law enforcement survey



# The Wrap

APEC has come a long way in 3 yrs

Now for more

**INFORMATION  
INTEGRITY  
SOLUTIONS**

**Malcolm Crompton**

Managing Director

53 Balfour Street

Chippendale NSW 2008

**+61 407 014 450**

[MCrompton@IISpartners.com](mailto:MCrompton@IISpartners.com)

[www.IISpartners.com](http://www.IISpartners.com)





Asia-Pacific  
Economic Cooperation

---

**2006/SOM1/ECSG/SYM/003**

Agenda Item: 1

## **APEC Information Privacy Framework (review, impact, and progress)**

Purpose: Information  
Submitted by: Australia



**APEC Symposium on Information  
Privacy Protection in E-Government  
and E-Commerce  
Ha Noi, Viet Nam  
20-22 February 2006**

**APEC Information Privacy Framework (review, impact,  
and progress) – Keynote speech**

***Malcolm Crompton***

**Managing Director, Information Integrity Solutions Pty Ltd; and  
Federal Privacy Commissioner of Australia, 1999-2004**

**APEC Symposium on Information Privacy Protection in  
E-Government and E-Commerce**

***Horison Hotel, Hanoi, 20-22 February 2006***

# **APEC Information Privacy Framework (review, impact, and progress)**

## **Introduction – purpose of this paper**

The purpose of this paper is to review briefly the history of privacy in an APEC context and outline the challenges of the future.

This is the third privacy seminar that APEC has sponsored. The first two seminars were held in June and September, 2005.

Many excellent papers were presented at the two seminars. They provide an excellent resource for business, policy makers and regulators operating in APEC Member Economies. These papers are available online at the following URLs:

Technical Assistance Seminar: Domestic Implementation of the APEC Privacy Framework, 1-2 June 2005, Hong Kong, China  
[www.apec.org/content/apec/documents\\_reports/electronic\\_commerce\\_steering\\_group/2005.html#SEMHK](http://www.apec.org/content/apec/documents_reports/electronic_commerce_steering_group/2005.html#SEMHK)

2nd Technical Assistance Seminar on Implementation of APEC Privacy Framework: International Implementation Issues, 5-6 September 2005, Gyeongju, Korea  
[www.apec.org/content/apec/documents\\_reports/electronic\\_commerce\\_steering\\_group/2005.html#SEM](http://www.apec.org/content/apec/documents_reports/electronic_commerce_steering_group/2005.html#SEM)

There is no need to repeat here the material presented in the papers presented to the first two seminars. Instead, this paper draws a brief road map through the issues and draws the attention of participants to relevant papers already presented.

## **Why is ‘Privacy’ on the APEC agenda?**

There is widespread recognition that a widely accepted and practical international standard of privacy protection is needed if e-commerce is to flourish.<sup>1</sup>

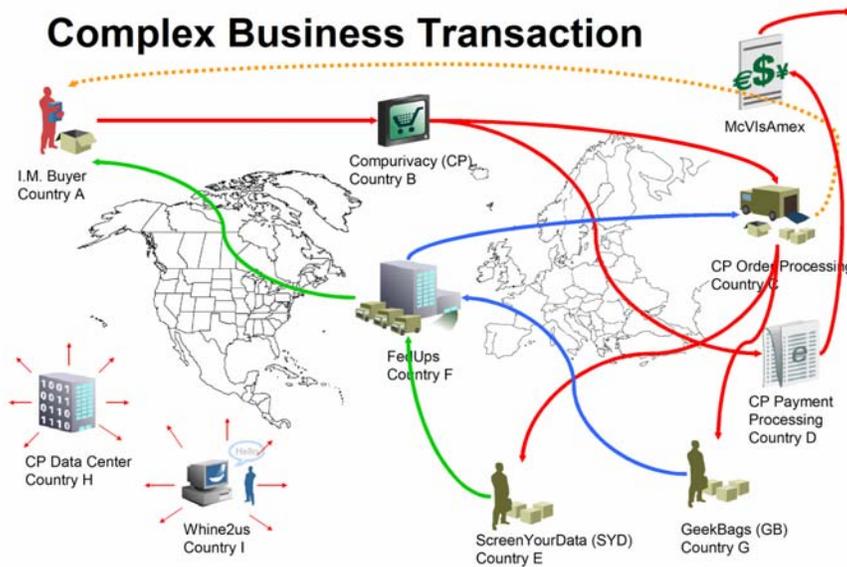
Today, flows of personal information can be rapid (or instantaneous), cross between the jurisdictions of many economies and be part of very complex transactions.

The following diagram was presented in the first Technical Assistance Seminar<sup>2</sup> to demonstrate this point.

---

<sup>1</sup> The underlying reasons are developed further in “APEC Privacy Framework: Facilitating Business and Protecting Consumers Across the Asia-Pacific” in APEC E-Newsletter Vol 7, January 2006, online at: [www.apec.org/apec/enewsletter/jan\\_vol7/onlinenewsd.html](http://www.apec.org/apec/enewsletter/jan_vol7/onlinenewsd.html)

<sup>2</sup> “Data Flows and Business Models: Distributing Information Flows and Business Functions”, Paper 2005/ECSG/SEM/005 presented to the 1<sup>st</sup> Technical Assistance Seminar and online at: [www.apec.org/apec/documents\\_reports/electronic\\_commerce\\_steering\\_group/2005/MediaLibDownload\\_v1.html?url=/etc/medialib/apec\\_media\\_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0103.File.v1.1](http://www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005/MediaLibDownload_v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0103.File.v1.1)



In 1998, when endorsing the 1998 Blueprint for Action on Electronic Commerce, APEC Ministers acknowledged that the potential of electronic commerce cannot be realised without government and business cooperation “to develop and implement technologies and policies, which build trust and confidence in safe, secure and reliable communication, information and delivery systems, and which address issues including privacy...”. The lack of consumer trust and confidence in the privacy and security of online transactions and information networks is one element that may prevent Member Economies from gaining all of the benefits of electronic commerce.

Almost everyone has a stake in privacy policy. Obviously, consumers are concerned to protect their personal information and business must be sensitive to the concerns of its customers. Governments have broad responsibilities for the social and legal environment in which commerce takes place, for encouraging electronic commerce and for safeguarding security, including law enforcement, within their societies.

Privacy policy cannot be considered in isolation but needs to take account of a range of twenty-first century problems such as identity fraud. It also needs to address the use of electronic technology to commit traditional crimes in novel ways.<sup>3</sup>

## A history of Privacy in APEC

Following workshops in Mexico in 2002 and Thailand in 2003, APEC Ministers endorsed the need to develop APEC data privacy principles. These principles are designed to help APEC Member Economies to develop privacy laws and regulations that achieve a balance between effective privacy protection and the continuity of cross-border information flows, thus promoting electronic commerce.<sup>4</sup>

<sup>3</sup> These thoughts are developed further in “APEC Privacy Framework June 2005 Domestic Implementation”, Paper 2005/ECSG/SEM/003 presented to the 1<sup>st</sup> Technical Seminar and online at: [www.apec.org/apec/documents\\_reports/electronic\\_commerce\\_steering\\_group/2005\\_MedialibDownload\\_v1.html?url=/etc/medialib/apec\\_media\\_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0101.File.v1.1](http://www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005_MedialibDownload_v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0101.File.v1.1)

<sup>4</sup> A brief history is also presented in “APEC Privacy Framework: Facilitating Business and Protecting Consumers Across the Asia-Pacific” in APEC E-Newsletter Vol 7, January 2006, online at: [www.apec.org/apec/enewsletter/jan\\_vol7/onlinenewsd.html](http://www.apec.org/apec/enewsletter/jan_vol7/onlinenewsd.html)

The development of the APEC Privacy Framework was given to a Data Privacy Subgroup of the Electronic Commerce Steering Group (ECSG) of the Senior Officers Meeting (SOM). The Subgroup completed the first part of this task in 2004 when APEC Ministers endorsed Part A of the APEC Privacy Framework.<sup>5</sup>

Part B of the Framework was completed and endorsed by Ministers in 2005.<sup>6</sup>

The Framework sets out a good, 'common practice' guide for Member Economies. Consistent with the APEC way, the Framework is aspirational, with individual Member Economies encouraged to develop ways of protecting personal information within an economy and when it moves between economies or is accessible in more than one economy.

## The APEC Privacy Framework

The complete APEC Privacy Framework is readily available online.<sup>7</sup> There are nine principles in the APEC Privacy Framework:

- Preventing harm
- Notice
- Collection Limitations
- Uses of Personal Information
- Choice
- Integrity of Personal Information
- Security Safeguards
- Access and Correction
- Accountability

These principles reflect and build on many of the privacy frameworks developed in other parts of the world. For example, all of the principles in one of the most widely respected frameworks, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data first published in 1980<sup>8</sup>, are reflected in the APEC Privacy Framework.

The way that the APEC principles work together is described extremely clearly in a paper presented to the first Technical Seminar in 2005.<sup>9</sup> In the simplest of terms:

---

<sup>5</sup> See "APEC Ministers Endorse the APEC Privacy Framework", Media Release, Santiago, Chile, 20 November 2004, online at: [www.apec.org/apec/news\\_media/2004\\_media\\_releases/201104\\_apecminsendorseprivacyfrmwk.html](http://www.apec.org/apec/news_media/2004_media_releases/201104_apecminsendorseprivacyfrmwk.html)

<sup>6</sup> See "Ministers Approve APEC Privacy Framework to Strengthen E-commerce and the Protection of Personal Information, Busan, Korea, 16 November 2005, online at: [www.apec.org/apec/news\\_media/2005\\_media\\_releases/161105\\_kor\\_minsapproveapecprivacyframework.html](http://www.apec.org/apec/news_media/2005_media_releases/161105_kor_minsapproveapecprivacyframework.html)

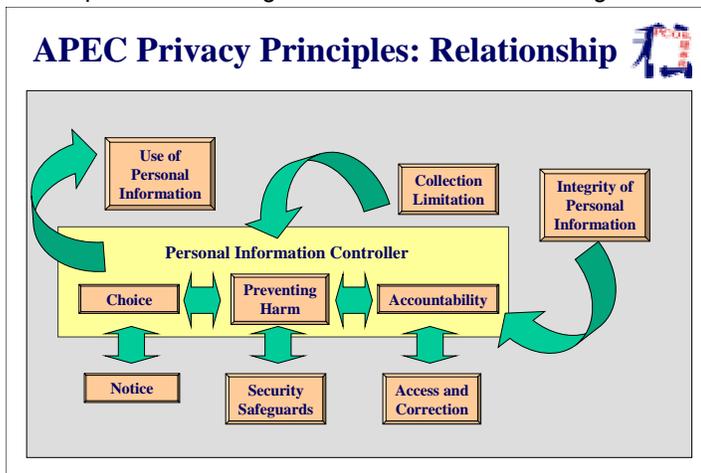
<sup>7</sup> The "APEC Privacy Framework" as endorsed by Ministers in November 2005 is online at: [http://203.127.220.112/content/apec/news\\_media/2005\\_media\\_releases/161105\\_kor\\_minsapproveapecprivacyframework.downloadlinks.0001.LinkURL.Download.ver5.1.9](http://203.127.220.112/content/apec/news_media/2005_media_releases/161105_kor_minsapproveapecprivacyframework.downloadlinks.0001.LinkURL.Download.ver5.1.9)

<sup>8</sup> The "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" endorsed by the Council of the Organisation for Economic Co-operation and Development (OECD) in September 1980 are available online at: [www.oecd.org/document/18/0,2340,en\\_2649\\_34255\\_1815186\\_119820\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_119820_1_1_1,00.html)

<sup>9</sup> "An Overview of the Principles Established by the APEC Privacy Framework" Paper 2005/ECSG/SEM/006, presented to the 1<sup>st</sup> Technical Seminar and online at: [http://www.apec.org/apec/documents\\_reports/electronic\\_commerce\\_steering\\_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec\\_media\\_library/downloads/taskforce/e CSG/mtg/2005/pdf.Par.0104.File.v1.1](http://www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/e CSG/mtg/2005/pdf.Par.0104.File.v1.1)

- An organisation that has control of personal information (the 'data controller') is required to handle that information in a way that prevents harm (Principle 1) and gives the individuals involved some choices about the uses of that data (Principle 5)
- A key component of preventing harm is that the data controller must also put in place security safeguards to protect the data (Principle 7)
- In order to give individuals choice, they must be given notice about the collection of the personal information (Principle 2)
- To be effective, the data controller is also held accountable for abiding by the privacy framework (Principle 9) and an important component of accountability is to provide individuals with access to information held about them and to correct any errors (Principle 8)
- Finally, as an input, the collection of personal information must be limited to information that is relevant to the purposes for which it is being collected (Principle 3) while there are corresponding limitations on output so that the personal information should only be used for the purposes for which it was collected (Principle 4).

This is presented in diagrammatic form in the following PowerPoint slide:<sup>10</sup>



[If reading this in Microsoft Word format, double click on the slide to see how each of the components link to each other.]

## The APEC insight

The APEC privacy framework is nevertheless different from other privacy frameworks such as the EU Privacy Directive in the way it protects personal information when it is being processed and in the way it provides for the free movement of such data<sup>11</sup>. These departures from other frameworks are crucial and seek to recognise the way personal information is already being handled and will be handled in the future. The key differences are to be found in Principles 1 and 9 of the Framework.

APEC Principle 1 extends the concept of proportionality that permeates a lot of thinking in the design of EU frameworks. In particular, it extends the concept of proportionality to apply in the

<sup>10</sup> In the Microsoft Word version of this document, double click on the diagram to see the way these components build up.

<sup>11</sup> The full title is "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data" and it is online at:

area of redress ('let the punishment fit the crime') so that it gives guidance to regulators in focusing their activities. To put it another way, the principle is an explicit recognition of the reality that most organisations, regulators or otherwise, have limited resources at their disposal and have to prioritise. The key will be to ensure an appropriately broad approach to the concept of 'harm' to ensure that it extends beyond immediate harm that is measurable only in financial terms to include other less tangible social harms some of which can be very hurtful.

Principle 9 is the most important innovation in the APEC Privacy Framework. In effect, this Principle is saying that 'accountability should follow the data'. Once an organisation has collected personal information, it remains accountable for the protection of that data. Just because personal information is passed on to another organisation or moves from one jurisdiction to another does not change that. Other frameworks tend to focus on border controls – in particular, whether the data moving from one jurisdiction which has 'adequate' data protection to another that has 'adequate' protection.

## Implementation of Privacy Principles – governance

When it comes to implementing the APEC Privacy Framework, it is always important to focus on the outcomes. The APEC Privacy Framework is seeking effective privacy protection that is efficient for business to implement. In the near future at least, the Framework will operate in the context of existing or imminent domestic privacy and other law.

Regardless of this position, the first and best approach to implementing any framework including the APEC Privacy Framework is for those directly handling the data to respect and abide by that framework on their own initiative. This means that good governance by individual businesses and government agencies is critical. Papers presented to the second Technical Assistance Seminar covered governance issues well.

First, the basic components of a good internal Privacy Governance Framework should include a number of components:<sup>12</sup>

- A high level policy
- Standard operating procedures
- Recommended measures and best practices
- Training ,communication and compliance tools
- Assurance functions

Second, there is good evidence that leading companies are working on putting good internal Privacy Governance Frameworks in place. In a survey of a select group of mostly US based companies with customers and data processing in the US and elsewhere, all had a privacy officer, other privacy staff and procedures. Most were able to ensure that their 'downstream' vendors etc were also meeting privacy requirements.<sup>13</sup>

---

[www.europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=quichett](http://www.europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=quichett)

<sup>12</sup> "Internal Privacy Governance Frameworks", Paper 2005/SOM3/ECSCG/SEM/010, presented to the 2<sup>nd</sup> Technical Assistance seminar, online at: [www.apec.org/apec/documents\\_reports/electronic\\_commerce\\_steering\\_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec\\_media\\_library/downloads/taskforce/ecscg/mtg/2005/pdf.Par.0080.File.v1.1](http://www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecscg/mtg/2005/pdf.Par.0080.File.v1.1)

<sup>13</sup> "Corporate Privacy Governance – A Prerequisite For APEC Implementation", Paper 2005/SOM3/ECSCG/SEM/011, presented to the 2<sup>nd</sup> Technical Assistance seminar, online at: [www.apec.org/apec/documents\\_reports/electronic\\_commerce\\_steering\\_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec\\_media\\_library/downloads/taskforce/ecscg/mtg/2005/pdf.Par.0081.File.v1.1](http://www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecscg/mtg/2005/pdf.Par.0081.File.v1.1)

Equally importantly, these companies are approaching governance in a multi jurisdiction context. They are doing this through internal networks and reporting structures. Their approach provides an example of how multi jurisdiction application of the APEC Privacy Framework might be enforced. For example, where such a company's internal Privacy Governance Framework meets the standards set by the APEC Privacy Framework, one option is for such companies to 'bind' themselves legally to abiding by that framework. To be 'binding', such an arrangement would have to be enforceable in law one way or another and include ways of addressing complaints by aggrieved individuals. This arrangement will not be practicable for the vast majority of companies operating in APEC, but it is an option for leading global corporations to show their bona fides as 'good corporate citizens'.

## Implementation of the APEC Privacy Framework – domestic

For some years now, an increasing number of Member Economies have implemented privacy law, many of them comprehensive and at the national level. Other economies have encouraged good practice codes in various ways.

The table below briefly summarises the situation.<sup>14</sup>

Country name	Privacy/Data Protection Law Status
<b>Australia</b>	<ul style="list-style-type: none"> <li>• Comprehensive national laws, National Privacy Principles (NPPs) and privacy codes and some state laws</li> <li>• Companies can gain approval of a code to replace the NPPs, which are then enforceable as law; codes must be 'at least the equivalent' of the NPPs</li> <li>• Independent Privacy Commissioner at federal level and some states enforces compliance</li> </ul>
<b>Canada</b>	<ul style="list-style-type: none"> <li>• Comprehensive national laws, provincial and territorial laws</li> <li>• Independent Privacy Commissioners at both federal and provincial levels enforce compliance</li> </ul>
<b>China</b>	<ul style="list-style-type: none"> <li>• No comprehensive law/regulations</li> <li>• Work on drafting has started</li> </ul>
<b>Hong Kong-PRC</b>	<ul style="list-style-type: none"> <li>• Comprehensive laws and codes of practices</li> <li>• Independent Privacy Commissioner enforces compliance</li> </ul>
<b>Indonesia</b>	<ul style="list-style-type: none"> <li>• No comprehensive law</li> <li>• Broad privacy right provision in the Electronic Transaction Bill</li> </ul>
<b>Japan</b>	<ul style="list-style-type: none"> <li>• Comprehensive national law, several guidelines and ordinances based on the law, prefectural and local laws</li> <li>• Responsible ministries/agencies enforce based on guidelines published respectively</li> </ul>
<b>Malaysia</b>	<ul style="list-style-type: none"> <li>• Drafted a comprehensive national data protection bill</li> <li>• The bill includes appointment of a Commissioner</li> </ul>

<sup>14</sup> The author takes responsibility for any errors in this table and apologises in advance for any such errors.

<b>Country name</b>	<b>Privacy/Data Protection Law Status</b>
<b><i>Mexico</i></b>	<ul style="list-style-type: none"> <li>• Data protection law only applicable to the government</li> <li>• Currently drafting a data protection bill that includes an appointment of a Commissioner</li> </ul>
<b><i>Philippines</i></b>	<ul style="list-style-type: none"> <li>• No comprehensive national laws</li> <li>• Currently developing data protection guidelines for the private sector</li> </ul>
<b><i>Singapore</i></b>	<ul style="list-style-type: none"> <li>• Voluntary private sector model code</li> <li>• Debating on whether to initiate legislation</li> </ul>
<b><i>South Korea</i></b>	<ul style="list-style-type: none"> <li>• Existing national law only applicable to certain industries</li> <li>• Currently drafting a restrictive data protection bill applicable to all industries</li> <li>• Currently compliance enforced by the Personal Information Dispute Mediation Committee which is supported by the Korea Information Security Agency</li> </ul>
<b><i>Taiwan</i></b>	<ul style="list-style-type: none"> <li>• Comprehensive national law</li> <li>• Bill with expanded scope submitted</li> </ul>
<b><i>Thailand</i></b>	<ul style="list-style-type: none"> <li>• Draft comprehensive national data protection bill under inter-agency review</li> </ul>
<b><i>U.S.A</i></b>	<ul style="list-style-type: none"> <li>• No comprehensive national laws, but sector-specific laws, state laws, and Federal Trade Commission law/regulations</li> </ul>
<b><i>Vietnam</i></b>	<ul style="list-style-type: none"> <li>• No comprehensive national laws</li> <li>• Privacy provision in the Electronic Transaction bill</li> </ul>

From a privacy perspective, the spread of privacy protection legislation must be welcomed where it is having material effect on improving individual privacy. However, inconsistencies between these laws make it more difficult for a business to operate across economies in the APEC region as the number of such laws grows. This has the potential to reduce the impact of the law in any one economy compared with what is possible with close harmonisation. Europe is already feeling the effects of insufficient harmonisation and continues to seek ways of alleviating them. On the other hand, individual Member Economies will continue to address data protection in ways that they see as appropriate to their circumstances and cultures. Respect for each economy's approach on these matters has been a key component of the APEC way.

In addition to putting in place privacy law, privacy codes or other mechanisms to encourage respect for privacy consistent with the APEC Privacy Framework, many economies also have programs to engage business and the public in helping them understand the privacy framework in place in their economy.

Implementation is likely to comprise a series of components such as:

- Engagement and Education
  - Making sure that individuals and organisations are aware of the issues and the benefits (including commercial benefits) of respecting individuals and the personal information about them

- Making sure that they are aware of good practice, relevant legislation and the APEC Privacy Framework
- Assistance to business and to government agencies when they face challenges in implementing the Framework
  - Consultation with officials and others should be based on solving problems not finding wrong doers when the business or organisation is clearly indicating good will and best endeavours
- Encouragement of low key, direct settlement of disputes between parties
  - Starting with effective, internal dispute resolution procedures
  - Low cost, credible alternative dispute resolution mechanisms provided by trusted public sector or private sector tribunals that are simple to use for all parties
- Enforcement
  - Always as a last resort
  - Always there as a credible threat in case all other options fail
  - Could involve one off or regular audits, official investigation of incidents
  - Includes remedies for the aggrieved party

## **Implementation of the APEC Privacy Framework – international**

As mentioned earlier, the APEC Privacy Framework is also intended to address the privacy of personal information when it moves between APEC Member Economies or is accessible in more than one economy.

Indeed, the seriousness of intent among Member Economies is best seen in the following extracts from Part B of the APEC Privacy Framework:

44. Taking into consideration existing international arrangements and existing or developing self-regulatory approaches (including those referenced in Part B. III., below), and to the extent permitted by domestic law and policy, Member Economies should consider developing cooperative arrangements and procedures to facilitate cross-border cooperation in the enforcement of privacy laws.
- .....
46. Member Economies will endeavor to support the development and recognition or acceptance of organizations' cross-border privacy rules across the APEC region, recognizing that organizations would still be responsible for complying with the local data protection requirements, as well as with all applicable laws. Such cross-border privacy rules should adhere to the APEC Privacy Principles.
  47. To give effect to such cross-border privacy rules, Member Economies will endeavor to work with appropriate stakeholders to develop frameworks or mechanisms for the mutual recognition or acceptance of such cross-border privacy rules between and among the economies.
  48. Member Economies should endeavor to ensure that such cross-border privacy rules and recognition or acceptance mechanisms facilitate responsible and accountable crossborder data transfers and effective privacy protections without creating unnecessary barriers to cross-border information flows, including unnecessary administrative and bureaucratic burdens for businesses and consumers.

This aspect is where APEC Member Economies still have the most work to do. In the near future at least, this will have to be developed in the context of existing or imminent domestic privacy and other law.

In broad terms, issues involved in implementing the APEC Privacy Framework at the international level will be legal, technical, or policy oriented.<sup>15</sup>

More specifically, mechanisms have to be found that ensure that when more than one jurisdiction is involved, the personal information neither suffers from more and more rules applying to it nor loses any of the protection it had when it was first collected. In other words, consistent with APEC Privacy Principle 9, accountability follows the data – no more, no less.

Building on the wording of Part B of the APEC Privacy Framework, there are a number of options for achieving this objective, including:

- A single, government backed authority such as an ‘APEC Privacy Commission’ that can engage, encourage, assist and enforce the Framework when more than one Member Economy is involved
- One or more Non Government Organisation (NGO) that offer similar services to an official ‘APEC Privacy Commission’<sup>16</sup>
  - Such bodies would need to work very hard to establish their authority and credibility
  - Government backing of some sort would almost certainly be essential to establish this authority and credibility
  - They would require subscribing organisations to commit to a set of Privacy Principles that meet the requirements of the APEC Privacy Framework, have suitable quality assurance processes in place and an easy to use dispute independent resolution mechanism
- Binding corporate rules
  - This is the approach foreshadowed earlier in the paper, under which a company would establish internal corporate rules that meet the requirements of the APEC Privacy Framework, and then legally ‘bind’ itself to those rules in an enforceable way
  - Enforcement mechanisms, including an independent dispute resolution, would need to be established
- A cooperative arrangement between the regulators in Member Economies who have responsibility for enforcing privacy standards for enforcing the APEC Privacy Framework in a way that makes sure that ‘accountability follows the data’ in such a way that personal information being handled in more than one jurisdiction neither suffers from more and more rules applying to it nor loses any of the protection it had when it was first collected.

This list is by no means exhaustive. Each Member Economy is also likely to have its own opinion on which option it prefers. However, for the APEC Privacy Framework to be credible for

---

<sup>15</sup> “Issues to be Considered in the International Implementation of APEC Privacy Framework”, Paper 2005/SOM3/ECSG/SEM/009 presented to the 2<sup>nd</sup> Technical Assistance Seminar and online at: [www.apec.org/apec/documents\\_reports/electronic\\_commerce\\_steering\\_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec\\_media\\_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0079.File.v1.1](http://www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0079.File.v1.1)

<sup>16</sup> A description of key requirements of such a body are set out in “Web Seals: A Review of Online Privacy Programs”, Paper 2005/SOM3/ECSG/SEM/008 presented to the 2<sup>nd</sup> Technical Assistance Seminar and online at: [www.apec.org/apec/documents\\_reports/electronic\\_commerce\\_steering\\_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec\\_media\\_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0078.File.v1.1](http://www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0078.File.v1.1)

personal information being handled in more than one jurisdiction, it will be essential to find some common ground.

There are some precedents and the beginnings of a solution emerging. For example, the *Privacy Act 1998* in Australia<sup>17</sup> allows a company or groups of companies to obtain approval for privacy codes that requires “at least the equivalent of all the obligations” set out in the National Privacy Principles established by the Act. Such codes then replace the National Privacy Principles and are enforceable under the Act. A code can also gain approval to have its own independent adjudicator.<sup>18</sup> In theory at least, similar legislation in other economies could allow a company to ‘join the dots’ between economies to get a single code approved. This is one possible mechanism to support Binding Corporate Rules or to support an NGO model.

Some of the privacy regulators in Member Economies have also begun informal discussion about the level of cooperation that they can undertake within their current legal frameworks. A survey of international data transfer provisions was also prepared for the 2<sup>nd</sup> Technical Assistance Seminar in 2005.<sup>19</sup> The US Federal Trade Commission also shared its experiences on resolving complaints in an international context, including its “SAFE WEB” proposals at the 2<sup>nd</sup> Technical Assistance Seminar.<sup>20</sup>

In addition to the direct work that APEC is undertaking on privacy, other APEC forums are addressing privacy in the work that they are doing such as the development of a Regional Movement Alert List (RMAL) multi-lateral framework.<sup>21</sup>

On a separate but related front, the Organisation for Economic Cooperation and Development (OECD) is about to conduct a survey cross-border co-operation in privacy law enforcement. OECD is very keen to include the responses of economies that are not members of OECD.

---

<sup>17</sup> The *Privacy Act 1998* is online at:  
[www.comlaw.gov.au/ComLaw/Management.nsf/current/bytitle/32AA97DFE9AA8326CA256F7100071D25?OpenDocument&VIEW=compilations](http://www.comlaw.gov.au/ComLaw/Management.nsf/current/bytitle/32AA97DFE9AA8326CA256F7100071D25?OpenDocument&VIEW=compilations)

The most relevant part of the Act is Part IIIAA ‘Privacy codes’, online at:  
[www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/bodylodgmentattachments/6BD809D508C0AF75CA2570CA0011DAF1?OpenDocument#para2.959](http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/bodylodgmentattachments/6BD809D508C0AF75CA2570CA0011DAF1?OpenDocument#para2.959)

<sup>18</sup> For more detail on privacy codes, adjudicators etc, see the Privacy Codes page of the Privacy Commissioner’s website at:  
[www.privacy.gov.au/business/codes/index.html](http://www.privacy.gov.au/business/codes/index.html)

<sup>19</sup> “A Survey of International Data Transfer Provisions in Existing Data Protection Legislation – Case Studies”, Paper 2005/SOM3/ECSG/SEM/005 presented to the 2<sup>nd</sup> Technical Assistance Seminar and online at:  
[www.apec.org/apec/documents\\_reports/electronic\\_commerce\\_steering\\_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec\\_media\\_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0075.File.v1.1](http://www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0075.File.v1.1)

<sup>20</sup> “Resolving Complaints In An International Context – FTC Experience with International Cooperation in Law Enforcement”, Paper 2005/SOM3/ECSG/SEM/012 presented to the 2<sup>nd</sup> Technical Assistance Seminar and online at:  
[www.apec.org/apec/documents\\_reports/electronic\\_commerce\\_steering\\_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec\\_media\\_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0082.File.v1.1](http://www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0082.File.v1.1)

<sup>21</sup> “Regional Movement Alert List (RMAL)”, Paper 2005/SOM3/CTTF/027 presented to the Counter Terrorism Task Force III meeting, 10-11 September 2005, Gyeongju, Korea, online at:  
[www.apec.org/apec/documents\\_reports/counter\\_terrorism\\_task\\_force/2005.MedialibDownload.v1.html?url=/etc/medialib/apec\\_media\\_library/downloads/taskforce/cttf/mtg/2005/pdf.Par.0087.File.v1.1](http://www.apec.org/apec/documents_reports/counter_terrorism_task_force/2005.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/cttf/mtg/2005/pdf.Par.0087.File.v1.1)

## Further work

At the end of the 2<sup>nd</sup> Technical Assistance Seminar, the Consultants to the Seminar tabled a report on the two seminars which was formally tabled at the ECSG meeting.<sup>22</sup> A copy of the Executive Summary of the report is set out in the [Appendix](#). The list of action items set out in the Executive Summary reflected all the work of the Seminar and the Data Privacy Subgroup. It presents a good starting point for further work by APEC on implementing its Data Privacy Framework over the next year or two.

Industry, regulators with privacy enforcement responsibilities and government policy makers will need to work together to deliver on the action list.

In one area in particular, there is willingness to pioneer a solution. Some leading global businesses want to establish corporate rules that apply the APEC Privacy Framework meaningfully. It has been suggested that the three key next steps for them to do so involve:

- a. Creating a checklist for industry accountability as a precursor for leading businesses to put together corporate rules that apply the APEC Privacy Framework
- b. Development of process for “approvals” of such rule sets
- c. Creation of international trust on enforcement of such rules

The achievements by APEC to date lay a very solid foundation for such pioneering work to be carried forward over the next year or two, right up to the point of actual implementation.

Further work could be identified in the Information Privacy Individual Action Plans that the Data Privacy Subgroup is considering asking Member Economies to complete. A draft template for such plans will be considered when the Subgroup meets on 22 February 2006.

Member Economies are strongly encouraged to participate in the OECD survey cross-border co-operation in privacy law enforcement. The survey and proposals for further cooperation have great potential to assist in improving the care of personal information world wide.

## Concluding remarks

Over the last three years since APEC commissioned the Data Privacy Subgroup to develop an APEC Privacy Framework, there has been remarkable progress. Working quietly in the background, this group has proceeded with great determination and great speed to cover a lot of ground. Rarely has a task as difficult as establishing a regional privacy framework been achieved in such a short time.

Moreover, Member Economies have already started discussing the implementation of the Framework at both the domestic and international levels, starting with the two Technical Assistance Seminars in 2005 and this Seminar at the start of 2006.

Member Economies have built a lot of momentum. The challenge now will be to maintain this momentum, including in finding the APEC way of respecting personal information when it is handled in more than one jurisdiction.

---

<sup>22</sup> “Final Report of the 2<sup>nd</sup> Technical Seminar on APEC Privacy Framework”, Paper 2005/SOM3/ECSG/021, tabled at the ECSG meeting of 8 September 2005, online at: [www.apec.org/apec/documents\\_reports/electronic\\_commerce\\_steering\\_group/2005\\_MediaLibDownload\\_v1.html?url=/etc/medialib/apec\\_media\\_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0047.File.v1.1](http://www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005_MediaLibDownload_v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0047.File.v1.1)

**Report of Second Technical Seminar on APEC Privacy Framework**

**Gyeongju, Korea**

**5-6 September 2005**

**Executive Summary**

This executive summary is submitted by consultants to facilitate discussion in meetings subsequent to the Seminar. It represents no more than the consultants own summing up of the lessons of the Seminar.

*Framework considerations*

- Consistent with the original mandate for developing the APEC privacy framework, focus on implementation models that facilitate international trade through the safe, efficient movement of personal information that is an integral component of business transactions
  - Recognise that in many economies, ‘privacy’ is not a strong public policy issue, with little public demand for action
  - Also recognise that for economies where there is a concern for the protection of personal information supported by legislative frameworks, they are seeking ways of protecting the personal information of their citizens when it is processed in other APEC economies
- Focus on accountability for personal information, wherever it happens to go, as the basis for safe, efficient flow of personal information between economies, consistent with Principle 9, rather than control of personal information at the point of it crossing the border from one economy to the next
- Framework action should recognise two complementary components
  - Governance
    - establishment of systems in businesses that demonstrably comply with APEC principles and the clearly articulated needs of regulators in particular, Business gets uniform rules for back end and can get compliance mechanism efficiently approved in the region
  - Remedy
    - Use of company complaint resolution processes as a first resort

Simple, effective remedy for consumers, preferably through a ‘one stop shop’ contact point in their own economy that does not depend on the consumer having to chase ‘data trails’

Regulator remains domestic authority but gains cooperation across borders

- ‘Think big; act small’ strategies
  - Develop solutions consistent with existing laws and mandates where possible

#### *Action Steps for the year ahead*

- Working groups of the Privacy sub group of ECSG be formed to carry forward work in particular areas including
  - Cooperation between developed and developing economies in the introduction of education and training programs
  - Cooperation among developed economies to explore mechanisms for compliance with the APEC Privacy Framework in cross-border transfers of information
  - Policy initiatives to find solution paths for business and government

Particular objectives that the working groups would facilitate should include:

- Continue outreach activities to those economies without their own privacy frameworks who are seeking to implement the APEC privacy framework, whether applied to domestic or international transfers of personal information
  - This might include seminars, workshops or developing educational resources and exchanges of policy information with key economy stakeholders such as policy makers, business and consumer groups
- A development program for staff of regulatory authorities with a focus on reaching a common understanding of the mandate of individual regulator/agencies
- APEC Privacy regulatory authorities develop more effective ways of consulting with each other, perhaps drawing on the ‘London Action Plan’ and methods of interaction developed in other forums such as ICPEN
  - All economies to identify agencies/regulators that need to be involved, if any
- Business, perhaps through representative bodies, to establish dialogue with regulatory authorities also acting in concert
  - Developing a stronger common understanding of global business information flows, drawing on the data flow modelling already under way
  - Focusing on internal governance and accountability

- Exploring the potential for non-government dispute resolution and trustmark bodies to contribute to efficient and effective governance and remedy arrangements
  - Clear government support for the action of these bodies may need to be considered
- Continued progress of Multi-Layered Privacy Notices in the APEC region
  - Complete and circulate “Ten Steps to an Effective Privacy Notice” as a collaborative effort between data protection authorities, consumer organisations and the private sector

*Action over the longer term*

- Economies to consider whether legislative change is needed to facilitate cooperative work between regulatory authorities
- Public engagement and education strategies, focusing on consumers and small business