Asia-Pacific
Economic Cooperation

2007/SOM1/ECSG/DPS/005

Report of First Technical Seminar on International Implementation of the APEC Privacy Framework

Purpose: Information
Submitted by: Information Integrity Solutions Pty Ltd

APEC
AUSTRALIA 2007

Data Privacy Subgroup Meeting
Canberra, Australia
24-25 January 2007

Report of First Technical Seminar on International Implementation of the APEC Privacy Framework

Canberra, Australia

22-23 January 2007

Introduction

The first technical seminar was held in Canberra, Australia on 22 and 23 January 2007. Some 16 economies were represented by over 100 delegates who attended.

Preparations for the seminar built on the conclusions reached by the Data Privacy Sub-Group at its meeting in Da Nang, Vietnam in September 2006. At that meeting, the Sub-Group agreed that one of the main goals of the APEC Data Privacy Subgroup work agenda for 2007 should be to develop options for pathfinder projects to be pursued in 2008.

The Data Privacy Sub-Group also considered that the best place to start in developing such options was to develop enforcement or oversight mechanisms that gave effect to Cross-Border Privacy Rules (CBPRs). Any option 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.

Purpose of the Seminar

The purpose of the seminar was to create a collaborative environment in which participants could consider options for putting in place a system for giving effect to CBPRs within the APEC Privacy Framework.

The work of the seminar is intended to provide useful input to the Data Privacy Subgroup's consideration of the challenges faced in developing a pathfinder project and moving towards implementation.

Structure of the Seminar

The seminar began by providing background and an 'environment scan' for participants during the first day. Then on the second day the seminar focused on three implementation models developed for discussion by the consultant to the seminar.

The approach to considering the implementation models was based on starting with a small number of APEC economies developing an efficient, enforceable compliance and complaints handling framework.

Three breakout groups then considered the options in detail. The seminar concluded with sessions that summarised these discussions in order to provide the input to the work of the Data Privacy Sub-Group.

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

The three models are also summarised in Appendix A.

Intended Seminar Outcomes

The Discussion Paper suggested specific Success Criteria for the models identified in the Discussion Models paper.

The first criteria come 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?

As noted in the Discussion Paper, it is important to note that the CBPR system being considered at this point is not seeking to improve domestic privacy protections within participating APEC economies.

Environmental Scan (Day 1)

Delegates were welcomed to the seminar by the Attorney-General of Australia, the Hon Philip Ruddock MP. He noted that what makes the APEC Privacy Framework distinctive is the focus on the practical implementation of consistent privacy protection within a regional context. He further noted that a key feature of the Framework is the need to maintain accountability in the flow of information among APEC economies and trading partners and that it is vital for business to have clear and simple ways of complying with basic principles for the protection of people's personal information.

The first session of the seminar provided an overview of the progress to date in developing an APEC Privacy Framework and the reason why this seminar is focused on cross-border data flows, with presentations from a leading business identity in the field of privacy, Joe Alhadeff from Oracle, from the Privacy Commissioner of Australia, Karen Curtis and an Australian Delegate to the Data Privacy Sub-Group, Colin Minihan.

Subsequent sessions helped participants gain an insight into business, consumer, regulator and policy maker perspectives on what they would like to see in a good cross-border privacy framework.

The consultant's summary of the points made by speakers during Day 1 and Day 2 of the seminar is set out in Appendix C.

Completing the Environment Scan and Testing the Discussion Models (Day 2)

The first substantive Session on Day 2 gave participants an insight into the perspective of businesses in the host economy, Australia. Transfer of bank data from New Zealand to Australia for processing then return to the original bank in New Zealand had resulted in Australian privacy law applying to that data as well as New Zealand data. The benefit to anybody of this additional compliance process was unclear. The challenge of aligning contract provisions that link elements of a value chain with cross-border regulatory processes was observed as a possible challenge.

In order to ensure that the seminar could draw on lessons learned in effective regulation in other arenas, leading Australian practitioners briefed participants on their experiences. The briefing on the Responsive Regulation framework and the 'Regulatory Pyramid' is based on moving up the scale of:

Capacity development > restorative justice > deterrence > incapacitation

The financial accounting and audit profession also has many lessons for appropriate data protection.

The remainder of Day 2 focused on the Discussion Models as planned. Each participant had the opportunity to participate in discussion on 2 of the 3 models in the Discussion Models.

When the Discussion Group leaders reported back there was a general view that Model 1, the "Choice of Approach" was the most promising, supported by elements of the Model 3 "APEC Region Trustmark". Model 2 "Council of Regulators" was seen as least promising.

Notes on the Discussion Leader reports are in Appendix B. The notes include a number of very specific observations and suggestions for next steps and these are summarized in the last slides of the consultant's daily summary in Appendix C. These observations include:

- Any model will need support of
  - Significant documentation, eg Standards expected in order for one economy to be able to trust the arrangements made by another; Instructions, Self Assessment templates for applicant businesses etc
  - Education for consumers, business, government

In summing up, David Loukidelis, Privacy Commissioner for British Columbia emphasized the importance of making a start. As noted earlier in the seminar, new insights into effective regulation include the importance of picking a fixable problem and fixing it, 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 summarized 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

Overall, participants agreed that a highlight of the seminar had been the breakout group work. Indeed, all agreed these sessions should have been longer in order to allow discussion of the models in greater depth.

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

As indicated from the title of the seminar, 'trust' is an important overarching theme to consider in implementing CBPRs. In considering the discussion models during the seminar, and in developing and for the purposes of refining proposals for practical implementation options following the seminar, participants were asked to bear the theme of trust in mind: trust between consumers and organisations; between consumers and regulators; between organisations and regulators; between regulators in different economies; and between organisations that transfer information to one another.

The level of trust that a CBPR system is able to incorporate within its processes will be important in determining whether or not the success criteria for the system can be achieved. It was noted several times during the seminar that, consistent with APEC Information Privacy Principle IX[1], 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.

While putting any framework in place will require genuine effort from interested economies, the general view was that it was well worth the effort.

[1] Principle IX provides: "A personal information controller should be accountable for complying with measures that give effect to the [APEC Information Privacy Principles]. When personal information is transferred to another person or organisation, 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 organisation will protect the information consistently with these Principles."

APPENDIX A

'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.

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.

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 B

Notes on Reports of Breakout Group Leaders

Group 1 – 'Choice of Approach' Model

Generally considered that this was a flexible model that all could fit with. General consensus that model could work but more structure needed around it, eg

- The structure of the self assessment form?
- What guidance would be given to companies doing the self assessment?
- How would consumers be educated about the meaning of an organization being APEC compliant?
- How would one economy know that a trustmark in another economy was satisfactory?
- Can we use a central website to coordinate a trustmark & use it for coordinating complaints? A good idea, though.
- Pathfinder needed to be implemented to test the model properly – a recurring theme on many questions.
- On the scorecard, each line got a 'yes', subject to various remarks about 'fleshing out'.
- But there were impediments, eg how to give any one economy strong reasons to trust the enforcement approaches of another economy;
- Businesses needed something to make it worth it to them to share information as needed to achieve compliance.
- Is forum shopping going to be a problem??
- Model will not achieve trust on its own. A lot of stakeholder education etc will also be needed
- On compliance review, does the model assist in designating compliant businesses? Again, how can one economy trust the designated authority of another. Each economy would have to work out how it designated its trust mark.
- Should be possible to base the rules on a template.
- Importance of linking the model to an enforcement entity in each participating economy. A problem of a government authority dealing with an NGO as the investigator in another economy, but may be it can be fixed by a MOU with the government regulator in that economy

Group 2 – Council of Regulators Model

There was not much support for this model, which was not the preferred model of most participants.

The biggest challenge would be the extent of structural development needed to implement it, with some economies having to legislate and create a suitable regulator. The problem was in structure of model not in what it sought to achieve.

The model was also not consistent with the APEC approach of accepting that each economy often took its own approach to resolving a commonly agreed challenge.

Specific thoughts on the 4 key areas:

1. There could be a significant resource challenge for regulators and the APEC secretariat
2. A lot of guidance would be needed on interpretation for business & consumers; again this has resource implications
3. On the other hand, the model creates strong oversight body but would the council have to meet formally in order to undertake assessments in a way similar to the EU's Article 29 Committee which could be too slow for business and when not all economies would have institutions with the capability to participate
4. Compliance costs – who pays; business would not want to meet the costs. Other questions included who acts on negative reviews; what would be the appeal process on negative decisions etc.
5. The model may work for big business but not small business.
6. Consumers may have more confidence in a government regulator
7. On recognition/acceptance, a published list of compliant business was probably a good idea, but what about any liability exposure for a regulator who signs off a business as compliant when it in fact had a problem?
8. First port of call should be respondent.
9. What would be the Council accountability within APEC? Would it be consistent with the APEC approach to institute such accountability mechanisms?
10. There may be a problem in finding a way of legally binding the businesses to the framework.
11. The model is probably not very flexible and not consistent with APEC approach of not creating bureaucracy

Group 3 – APEC Region Trustmark Model

Arguably, a pure trustmark model is not possible in the APEC context. However, a Trustmark concept is likely to be a great first step for an economy without privacy law. Some might see it as a lower standard, but it need not be.

The answer to whole of the breakout session scorecard is 'yes – but'.

The but's include:

- The assumption that all of the framework has been worked out.
- Government involvement – even if the trustmark is private sector driven and driven hard, there must be a regulator in the background to back it up. On the other hand, don't assume consumer trusts government in all economies, so direct consumer involvement needed in the trustmark process.
- Who sets the quality control of the whole system?
- Will the sanctions be there and enforced? Will this included name names?

- Who is going to pay for it? There is great benefit if all stakeholders meet some of the costs
  - Eg regulator now hasn't the resources for all the work while the trustmark model allows somebody else to do some of the work; can even put in some additional layers to refine the process

- What about economies without trustmarks? Maybe a solution is to allow for a trustmark in another economy to offer the service, with a national trustmark council of regulators and business folk to decide who is an acceptable trustmark

- What about the clash of the regulatory frameworks. Privacy is very culturally oriented; there is not even a word for privacy in Chinese language.

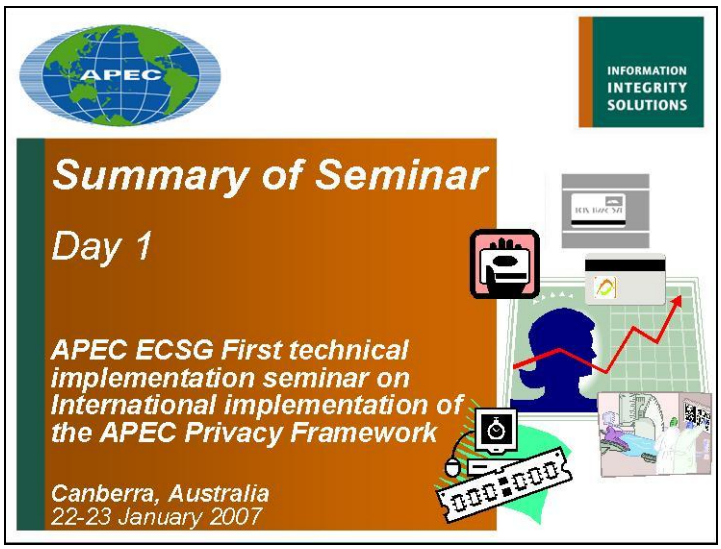
- General consumer protection law can fill the gap for this framework in some economies.

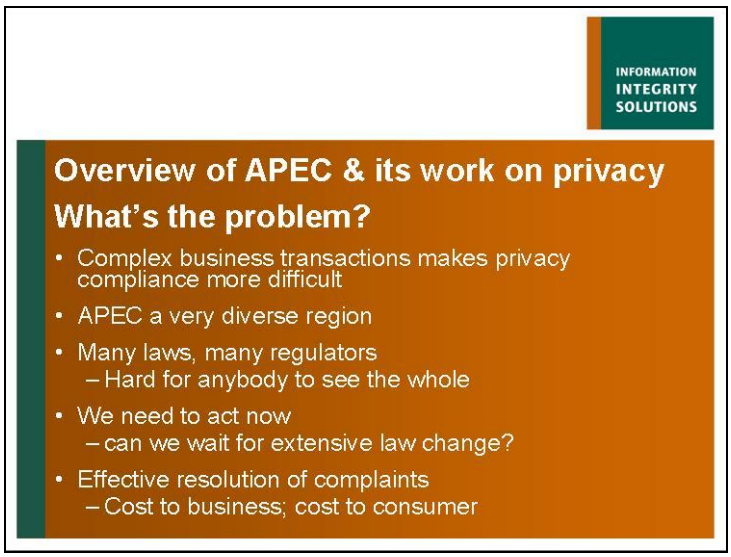
- In the end, the advantage of the pathfinder process is that it helps undertake a large process step by step.

- Quite a consensus for an approach based on blending the best from each model.

APPENDIX C

Daily Summaries of the Seminar by Consultant





INFORMATION INTEGRITY SOLUTIONS

LIMITED first steps

- APEC's ECSG Data Privacy Sub-Group wants to address a small part of the problem in pathfinder projects in 2008
  - Consumer to business (& business to business) only
  - A volunteer group of APEC economies only
  - Cross-Border Privacy Rules only
  - For Businesses that opt in only
  - Hence, probably large companies only
- Expand later if successful
  - Start again if not successful ?!?
- Remember this integrates into wider Sub-Group work eg on information sharing & cooperation between regulators

INFORMATION INTEGRITY SOLUTIONS

We can do this!

- Win-Win-Win is possible
  - Good privacy is good business
  - But flexibility needed in a region as diverse as APEC
  - Time to develop detailed requirements; get beyond theory
  - Need transparency, consistency, user friendly systems and credible accountability across borders
- Regulator cooperation in the region has commenced
  - APPA – Asia Pacific Privacy Authorities
  - MOU between Australia and New Zealand

INFORMATION INTEGRITY SOLUTIONS

A business perspective

- Take in, use, move & share data to fulfil operational goals
- Worldwide consistency in operations
- Eliminate conflicting contradictory legal requirements
- Minimise cost & maximise efficiency
- Preserve trust
- Model 1 preferred
  - Can establish a substantive floor
  - Requires least change of domestic law
  - But who pays for compliance processes?

INFORMATION INTEGRITY SOLUTIONS

Another business perspective

- Time for business privacy policies to reflect current technologies & business practices
  - Including those who act as 'agents', eg travel agents for airlines & hotels
  - Some agents simply hold the data but are not able to read it or use it
  - ie focus on personal information as it moves along value chain
- Vendor should fit into CBPR even though they themselves do not collect the personal information
  - Incorporate into existing Information Security Management Systems (ISMS)

INFORMATION INTEGRITY SOLUTIONS

A consumer perspective

- A cautious welcome to this initiative; a useful entry point
  - CBPRs should only supplement domestic privacy rules
  - eg self assessments should include self assessment against domestic law, eg domestic data export rules
- Clarify whether CBPRs cover
  - consumer to business; business to business; or also
  - consumer to government; government to government etc
- Some potential downsides to implementation models
  - Could cost regulators & businesses more than expected
  - Will CBPRs assist small to medium business?
  - Will CBPRs deal with bad guys as well as good guys?

INFORMATION INTEGRITY SOLUTIONS

Some policy perspectives

- Divide the world into economies with privacy law & those without
  - MOUs between economies with similar privacy law?
  - For other economies, consumer consent needed before transfer
- Possible to use consumer protection law to protect privacy
  - eg Mexico Trustmark funded by Ministry of Economy & based on Agreement between Ministry, Consumer Protection Authority (Profeco) & Mexico internet society, (AMIPCI)
  - Based on APEC Privacy Framework

INFORMATION INTEGRITY SOLUTIONS

A regulator perspective

- Lack of jurisdiction on complaints already happening
  - A range of solutions needed involving great flexibility, including MOUs
  - Some sharing of data on investigations with regulators in other economies has proved possible
- Consumer protection law already used effectively in one economy
  - Considered possible to do the same for CBPRs

INFORMATION INTEGRITY SOLUTIONS

Lessons learned & emerging privacy law

- Protection of personal information when it moves between economies is a very new concept
- China for example still has to think this through
  - Little legal foundation in domestic law at present
  - Huge domestic issues to address
- US-EU Safe Harbor program has many of the components of a possible APEC CBPR implementation framework
  - Assurance process before commit to Safe Harbor
  - Annual assurance process
  - Complaints handling part of process

APEC has come a long way in 3 yrs

Now for more

INFORMATION INTEGRITY SOLUTIONS

Summary of Seminar

Day 2

APEC ECSG First technical implementation seminar on International implementation of the APEC Privacy Framework

Canberra, Australia
22-23 January 2007

INFORMATION INTEGRITY SOLUTIONS

Australian business perspectives

- Bank transfer of data from New Zealand to Australia for processing then return to original bank
  - Hence Australian privacy law also applies to the data as well as New Zealand law
  - Additional compliance costs for little consumer benefit
- Data breaches occur in all economies, with or without privacy laws
- Increasing number of players in a value chain
  - Contractual arrangements important but little guidance & enforcement a challenge
  - Challenge of appropriate notice to consumers

INFORMATION INTEGRITY SOLUTIONS

Australian business perspectives (cont)

- If contract underpins links in a value chain, how are they written to support investigation by the regulators in affected economies
  - Hence Australian privacy law also applies to the data as well as New Zealand law
- 'Devil in the detail' examples
  - eg, the challenge of ensuring consistent Regional Privacy Policy development

INFORMATION INTEGRITY SOLUTIONS

What's happening elsewhere?

- Under regulation & over regulation can be equally harmful
- Responsive Regulation
  - Capacity development > restorative justice > deterrence > incapacitation
  - Start with the simple, cheap, polite
  - Be able to advance up 'regulatory pyramid' to more & more intrusive, less & less focused only on 'learning'
- Success from story building, not procedure manual
  - Reward what goes right – continuous improvement
  - Not a 'rights' discourse or a 'blame culture'
- Triple loop learning

INFORMATION INTEGRITY SOLUTIONS

What's happening elsewhere? (cont)

- Seal programs in the APEC region
  - Industry specific or purpose specific
  - Asia Trustmark Alliance
- Some key characteristics of Seal programs
  - Government-certified in some way
  - Participants self assess then Seal verifies in some way
  - Regular ongoing assurance process
  - Complaints handling processes
- Financial accounting and auditing has many lessons for us
  - Including movement from co-regulation & principles based regulation to more government intervention & rule writing after notable failures

INFORMATION INTEGRITY SOLUTIONS

Assessment of Discussion Models

- Important to make a start
  - Pick a Fixable Problem and Fix it & begin a process of confidence building
- 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

INFORMATION INTEGRITY SOLUTIONS

Assessment of Discussion Models (cont)

- General view that Model 1 "Choice of Approach" the most promising, supported by elements of the Model 3 "APEC Region Trustmark"
  - Model 2 "Council of Regulators" seen as least promising
- Any model will need support of
  - Significant documentation, eg Standards expected in order for one economy to be able to trust the arrangements made by another; Instructions, Self-Assessment templates for applicant businesses etc
  - Education for consumers, business, government
- Unclear how much law change needed in any one economy wanting to participate
  - Not always much? could trustmark approach ease it?

INFORMATION INTEGRITY SOLUTIONS

Assessment of Discussion Models (cont)

- Don't forget resource challenge
  - For development of pathfinder
  - For implementation of pathfinder
  - May need imaginative approach – spread the load: government, business, regulator, consumer
- If Data Privacy Sub-Group wishes to proceed with 2008 pathfinder, need to progress before Cairns Mtg in June

INFORMATION INTEGRITY SOLUTIONS

Assessment of Discussion Models (cont)

- Steps to start before Cairns include:
  - shape the pathfinder; APEC Business Card an example: started with 3 economies; now 17 participate; strong continuous evaluation process in place etc
  - Participating economies to analyse any law change needed
  - Ensure all relevant regulators in APEC informed & engaged
  - Convene group to begin drafting some of the instruments, perhaps comprising partnership between CBPR study group and Regulators, Academics, Trustmark interests


INFORMATION
INTEGRITY
SOLUTIONS
Malcolm Crompton
Managing Director
53 Balfour Street
Chippendale NSW 2008
Australia
+61 407 014 450
MCrompton@iispartners.com
www.iispartners.com