HIDE

INFORMATION INTEGRITY SOLUTIONS

Malcolm Crompton

Trust, Transparency & data Governance: Challenges in the APEC privacy framework & the EU directive

APEC

HIDE Workshop on International data sharing & Biometric identification: Ethical Issues in an Asian & International Context

Singapore
2 July 2008

Why is ‘Privacy’ on the APEC agenda?

INFORMATION INTEGRITY SOLUTIONS

Overview of APEC & its work on privacy

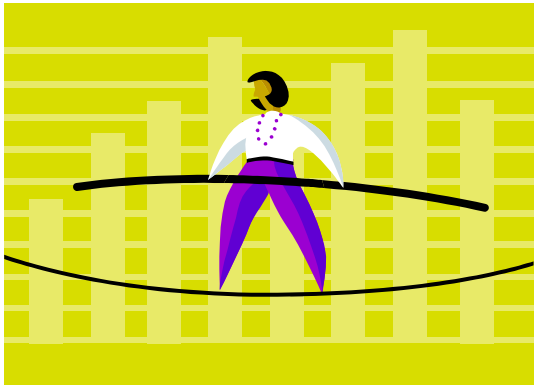
The problem:

- Complex business transactions makes privacy compliance more difficult
- APEC a very diverse region
- Many laws, many regulators
  - Hard for anybody to see the whole
- We need to act now
  - can we wait for extensive law change?
- Effective resolution of complaints
  - Cost to business; cost to consumer

INFORMATION INTEGRITY SOLUTIONS

The objective:

- "Privacy is local; processing is global"
- How to keep the original privacy promise comprising:
  - Original economy law
  - Company privacy policy and other undertakings
  - Consumer choices
- In short: eliminate additional "country risk" for the individual



INFORMATION INTEGRITY SOLUTIONS

Asia Pacific privacy law – summary position

Omnibus or sector law	Minimal privacy law
USA *	China #
Canada *	Singapore #
Japan	Malaysia #
Korea *	Thailand #
Hong Kong *	Mexico #
Australia *	Chile
New Zealand *	India
Taiwan	Indonesia
Russia	others

APEC Privacy Principles

* With enforcement

\# Law under consideration

The APEC Privacy Framework

INFORMATION INTEGRITY SOLUTIONS

Nine APEC privacy principles

1. Preventing Harm – privacy protections should focus on preventing harm and misuse
2. Notice – clear & easily accessible (cf EU Dir Art 10, 11)
3. Collection Limitation – collect what's relevant in a lawful & fair manner after notice or consent (cf EU Dir Art 6)
4. Uses of Personal Information – for expected and compatible purposes, with consent, or where necessary (cf EU Dir Art 7)
5. Choice – where appropriate, provide clear, accessible mechanism to exercise choice (cf EU Dir Art 8, 14)

INFORMATION INTEGRITY SOLUTIONS

Nine APEC privacy principles

6. Integrity – personal information should appropriately accurate, complete and up-to-date (cf EU Dir Art 6)
7. Security – appropriate safeguards to protect against unauthorized access, use, modification or disclosure (cf EU Dir Arts 16, 17)
8. Access & Correction – important (but not absolute) rights (cf EU Dir Art 12)
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

INFORMATION INTEGRITY SOLUTIONS

APEC Privacy Framework & EU Data Protection Directive 95/46/EC

Similarities

- EU Privacy Principles generally map into APEC Privacy Principles although:
  - sensitive information not called out so specifically as EU Dir Art 8
  - right to object to processing not spelt out cf EU Dir Art 14
  - protection against ‘automated decisions’ EU Dir Art 15
- Significant variations in transposition into national laws

INFORMATION INTEGRITY SOLUTIONS

APEC Privacy Framework & EU Data Protection Directive 95/46/EC

Differences

- Enforcement frameworks and approaches – process or outcomes?
- Transborder data flows
- The APEC insight...

INFORMATION INTEGRITY SOLUTIONS

Insight in Principles 1 & 9

Principle 1

- Proportionality: focus effort on where harm greatest

Principle 9

- ‘Accountability follows the data’

Implementation

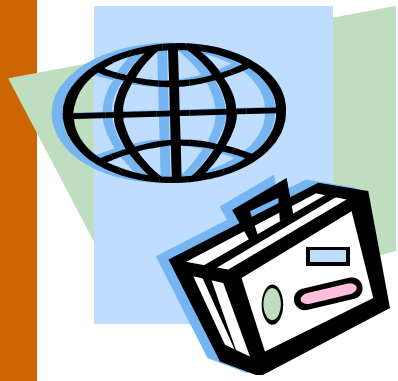
INFORMATION INTEGRITY SOLUTIONS

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."



INFORMATION INTEGRITY SOLUTIONS

LIMITED first steps on cross border

- APEC's ECSG Data Privacy Sub-Group addressing a small part of the problem in pathfinder projects
  - 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

The APEC CBPR System

- CBPR system has 4 elements:
  - self-assessment; compliance review; recognition; dispute resolution & enforcement
- Pathfinder implemented through 8 projects
  - address the 4 elements
  - 9th project tests the outcomes
- 'Rules' not formal or imposed but when adopted will be enforced:
  - refers to internal procedures developed & used by business
  - must satisfy minimum requirements of APEC privacy principles

INFORMATION INTEGRITY SOLUTIONS

The APEC Data Privacy Pathfinder

- The Data Privacy Pathfinder was endorsed by Ministers in Sydney in September 2007
- It focuses on achieving accountable cross-border information flows
  It requires: conceptual framework; consultative processes; practical documents; implementation strategies; and education and outreach
- Aim: to protect personal information no matter where in the APEC region the personal information is transferred or accessed

INFORMATION INTEGRITY SOLUTIONS

Pathfinder pilots for CBPR

- Self-assessment guidance for organisations
- Guidelines for accountability agents
- Compliance review of an organisation's CBPRs
- Directory of compliant organisations
- Data Protection Authority & Privacy Contact Officer Directory
- Enforcement Cooperation Arrangements
- Template cross-border complaint handling form
- Governance model
- Cross-Border Privacy Rules International Implementation Pilot Project

Implementation:

As important as the rules

INFORMATION INTEGRITY SOLUTIONS

“Layered Defence” essential

Privacy ► Control ► Trust ► Risk ► Accountability

Education

Law

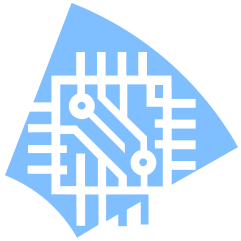
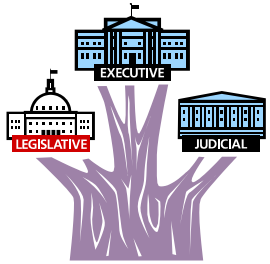
Technology

Governance

Safety Net

We can reduce the Trust Deficit



INFORMATION INTEGRITY SOLUTIONS

Layered Defence tools

"**Business as usual**" – good practice & culture change for staff & citizen users

Law – maybe more, where risks particularly high (eg specific use and disclosure limitations, criminal penalties, special measures to ensure review before critical changes made); NOT just compliance

Technology – design limits information collected, what can be connected and who can see what

Governance – including transparency and accountability

Safety mechanisms for citizens when failure or mistakes occur

INFORMATION INTEGRITY SOLUTIONS

Effective enforcement across borders

- Accountability the key
  - "original collector of the personal information remains accountable for compliance with the original privacy framework that applied when & where the data was collected, regardless of the other organisations or countries to which the personal data travels subsequently"
  - "The Australian *Dodo* Case: an insight for data protection regulation" where ACMA applied this principle

Crompton et al, World Data Protection Report, Vol 9, No 1, Jan 2009
www.iispartners.com/Publications/index.html#Other2009

- Regulator cooperation
  - Legal, Financial, Moral mandates

INFORMATION
INTEGRITY
SOLUTIONS

Malcolm Crompton
Managing Director

53 Balfour Street
Chippendale NSW 2008
Australia

+61 407 014 450

MCrompton@iispartners.com
www.iispartners.com