INFORMATION INTEGRITY SOLUTIONS

Interoperability effort between APEC CBPR and EU BCR

Malcolm Crompton
Managing Director, IIS

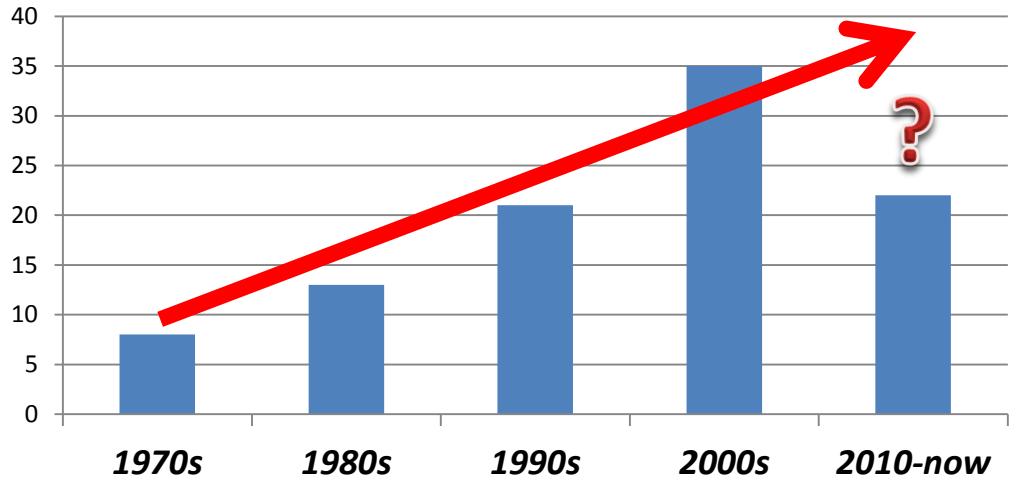
Google Japan

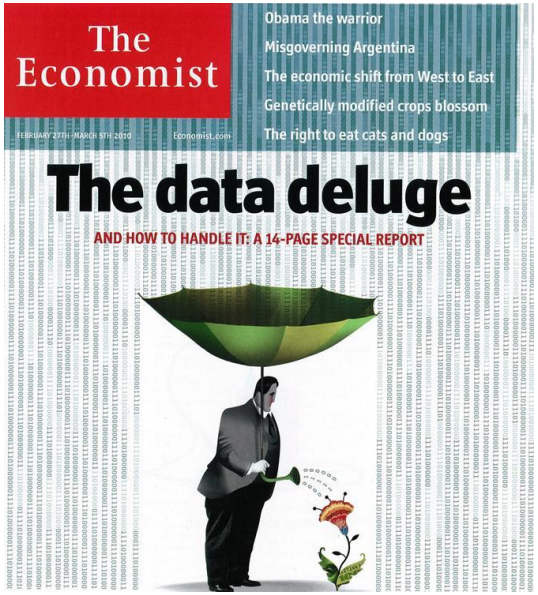
Tokyo, 17 April 2014

INFORMATION INTEGRITY SOLUTIONS

The case for a global interoperability framework

- Privacy laws are proliferating





- Cross-border data flows are accelerating
- Protecting personal data requires international cooperation
  - EU – Largest economic entity in the world
  - APEC – 40% of world's population, 54% of world's GDP, 40% of world trade

Building trust and innovative privacy solutions

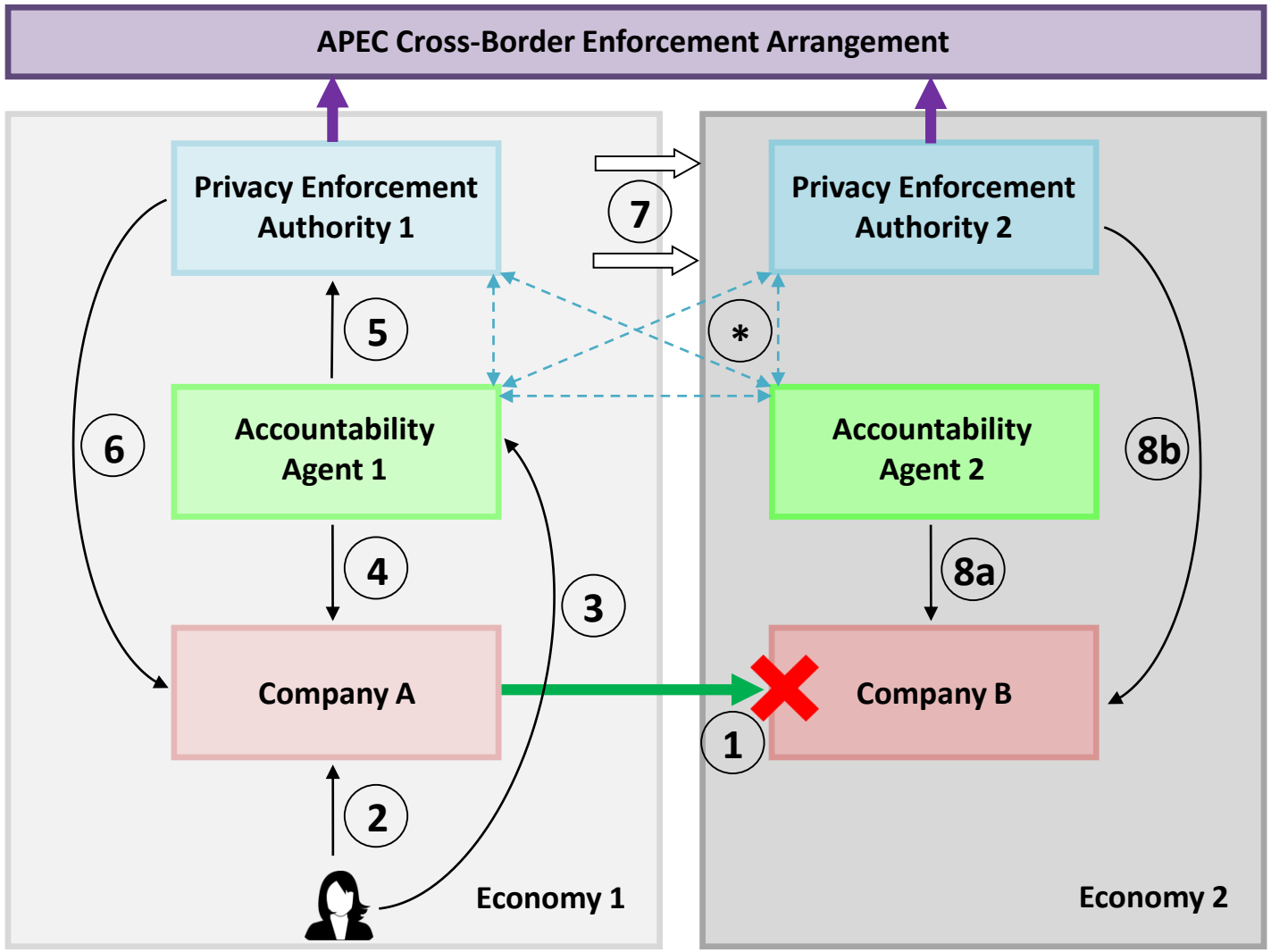
INFORMATION INTEGRITY SOLUTIONS

EU BCR
&
APEC CBPR

Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

APEC Cross-Border Privacy Rules System



1. Personal information is transferred to Company B and a privacy breach occurs

2. Complain directly to Company A

3. If no resolution, complain to AA 1

4. Enforcement by AA 1

5. If no resolution, escalate to PEA 1

6. Enforcement by PEA 1

7. If no resolution in Economy 1, refer complaint to AA 2 and/or PEA 2 in Economy 2

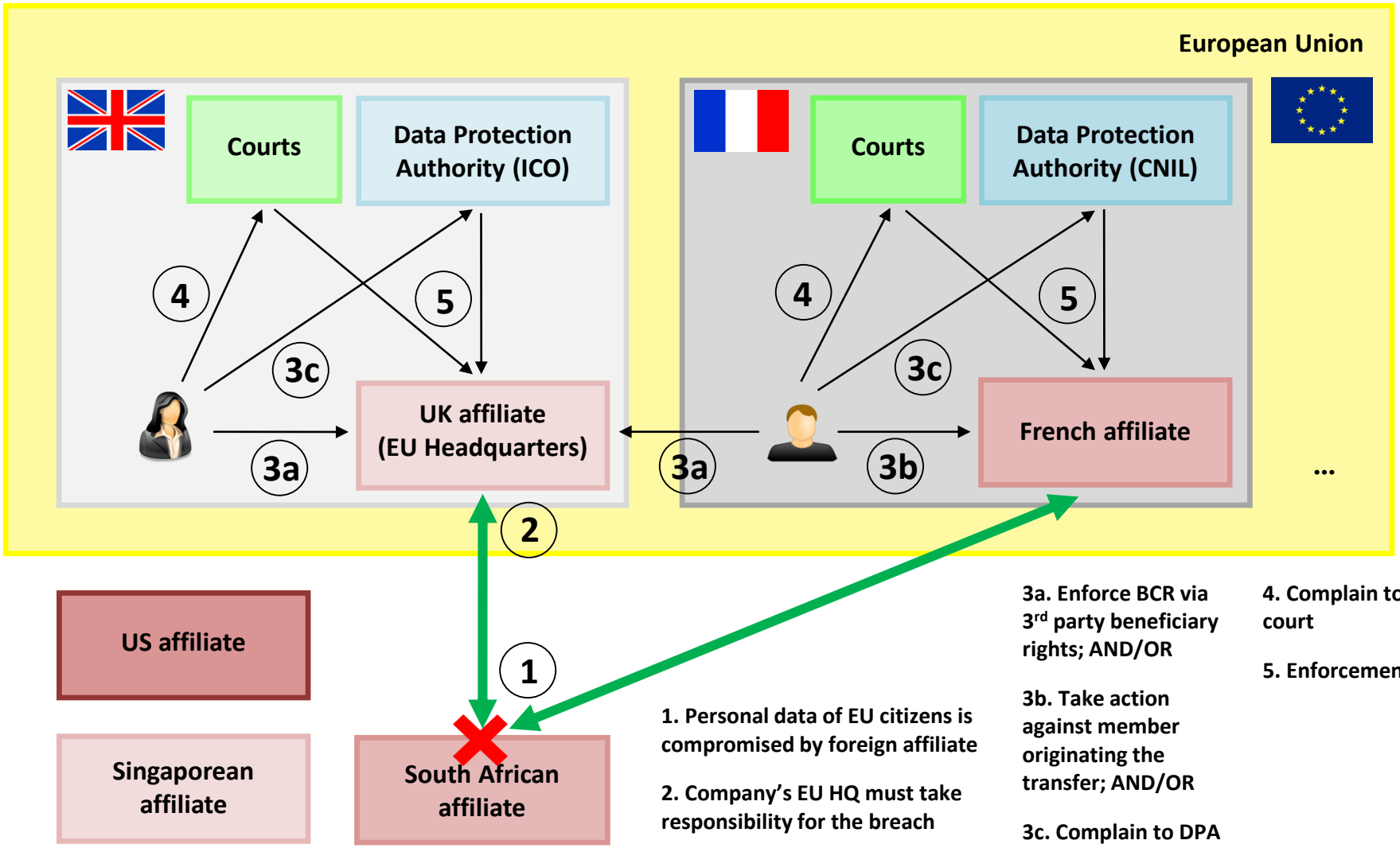
8a. Enforcement by AA 2

8b. Enforcement by PEA 2

* Cooperation where appropriate and possible

INFORMATION INTEGRITY SOLUTIONS

EU Binding Corporate Rules



INFORMATION INTEGRITY SOLUTIONS

Towards global interoperability: incremental steps

- Regional, not global solutions, so far
- Different scope of operation:
  - CBPR – transfers between participating companies in participating Economies (geography)
  - BCR – intra-company transfers (corporate structure)
- IIS Comparison and Assessment Sep 2013
- Referential (27/02/14) outlines separate and **overlapping** requirements
  - Double certification, not interoperability

INFORMATION INTEGRITY SOLUTIONS

Key elements

1. A baseline level of **privacy protection that follows the data**
2. Expressed through **internal rules and policies**
3. Enforced via **accessible redress mechanisms** when something goes wrong
4. Demonstrated through **initial certification and ongoing audit**

INFORMATION INTEGRITY SOLUTIONS

1. Privacy protection...

- Common principles:
  - Fair and lawful collection
  - Purpose specification
  - Notice and transparency
  - Data quality
  - Data security
  - Rights of access, correction and deletion
  - Choice
- EU-specific:
  - Retention limitation
  - Restrictions on processing of sensitive information
  - Right to object to automatic processing

INFORMATION INTEGRITY SOLUTIONS

1. … that follows the data

- Common features:
  - Only transfer data to other organisations that will apply the same protections
  - One entity accepts responsibility
  - Mutual assistance and cooperation between DPAs/PEAs (in the EU and APEC respectively)

INFORMATION INTEGRITY SOLUTIONS

2. Internal rules and policies

- Common features:
  - Application to group entities and third party processors
  - Designate individual(s) to be responsible for privacy within organisation
  - Privacy training program for employees
- EU-specific:
  - Explicit requirement for employees to be bound by internal rules and policies

INFORMATION INTEGRITY SOLUTIONS

3. Redress mechanisms

- Common features:
  - Formal process within organisation for handling of privacy complaints
- EU enforcement avenues:
  - Judicial remedy
  - Data Protection Authority
- APEC enforcement avenues:
  - Accountability Agent and dispute resolution process
  - Escalate to Privacy Enforcement Authority where necessary
  - Private right of action (depending on local law)

INFORMATION INTEGRITY SOLUTIONS

4. Demonstrate compliance

- Common features:
  - Participation requirements assessed and certified by relevant body (DPA / Accountability Agent)
  - Ongoing monitoring and audit
- EU-specific:
  - Audit on regular basis, by internal or external party
  - Provide copy of audit to DPAs on request
  - DPAs may audit and issue binding advice
- APEC-specific:
  - Regular monitoring of processors/agents/contractors/other service providers to ensure compliance with instructions
  - Attest continuing adherence to CBPR program requirements on annual basis
  - Accountability Agents to conduct regular comprehensive reviews

INFORMATION INTEGRITY SOLUTIONS

The Australian approach

- Flexible, enforceable, adaptable to BCR & CBPR schemes
- Privacy Act 1988 – updated in 2014
- 13 Australian Privacy Principles – replaced/upgraded existing principles
  - Similar to APEC and EU principles – a good platform for BCR & CBPR
  - Changes included:
    - New, clear obligation to demonstrate steps to comply, eg policies, procedures
    - Concept of anonymity and 'pseudonymity' at collection – don't collect, or collect minimal details, ID where practical
    - De-identified (including anonymous) personal information not subject to Act
      - Adequate de-identification recognised as difficult – identity often quickly apparent
      - See Australian advice on de-identification
    - Reform of cross-border transfers, introducing 'accountability' obligation, following data, unless other protection in place

INFORMATION INTEGRITY SOLUTIONS

Australian approach cont.

- Privacy Act changes include new powers to assess compliance and new, tougher enforcement options, enforceable undertakings & penalties up to $1.7m
- Regulator's approach – more effort on individual resolutions, education. Tougher sanctions used sparingly for egregious matters
- Organisations/sectors permitted to self-regulate via codes
  - Codes must meet standards, be registered, are enforceable
  - A platform for BCR, CBPR

INFORMATION INTEGRITY SOLUTIONS

What now?

- Opportune time for Japan:
  - Vision – Declaration to be the World's Most Advanced IT Nation (2013)
  - Nationally – legal and institutional privacy reform
  - Internationally – participation in CBPR system
- Demand Internationally for interoperable and enforceable frameworks continues to grow

Questions?

INFORMATION
INTEGRITY
SOLUTIONS

Malcolm Crompton
Managing Director

53 Balfour Street
Chippendale NSW 2008
Australia

+61 407 014 450

MCrompton@iispartners.com
www.iispartners.com