



**Asia-Pacific
Economic Cooperation**

2013/SOM1/ECSG/DPS/II/005

Agenda Item: II

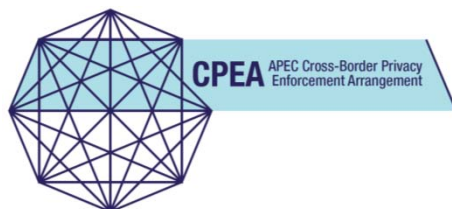
APEC's Cross-border Privacy Enforcement Arrangement: A Case Study in Interoperability

Purpose: Information
Submitted by: New Zealand



**Data Privacy Subgroup Informal Meeting
Jakarta, Indonesia
31 January 2013**

APEC's Cross-border Privacy Enforcement Arrangement: A Case Study in Interoperability



Blair Stewart
Assistant Privacy Commissioner, New Zealand

First meeting of joint working team between the ECSG Data Privacy Subgroup and the EU Article 29 Working Party
Jakarta, 31 January 2013

Presentation overview



- What is interoperability?
- Background to development of CPEA – with particular focus on interoperability objectives
- Outline of CPEA – with particular focus on aspects relevant to interoperability objectives
- The future of CPEA – CBPR, review, new environment

APEC Cooperation Arrangement for
Cross-border
Privacy Enforcement (CPEA)



- A multilateral arrangement [MOU] that creates a practical mechanism for privacy enforcement authorities to cooperate in a cross-border environment
- “CPEA signifies the on-going commitment within APEC to increase the protection of cross-border flows of personal information and is a significant step in the effective implementation of the APEC Privacy Framework”
- “The CPEA aims to contribute to consumer confidence in electronic commerce involving cross-border data flows ...”
- “The CPEA is an outcome of the Pathfinder initiative. It focuses on one of the four key goals of the APEC Privacy Framework, namely to facilitate both domestic and international efforts to promote and enforce information privacy protections ...”

What is Interoperability?



What is interoperability?



Interoperability

From Wikipedia, the free encyclopedia

Interoperability is the ability of diverse systems and organizations to work together (inter-operate). The term is often used in a technical [systems engineering](#) sense, or alternatively in a broad sense, taking into account social, political, and organizational factors that impact system to system [performance](#).

While **interoperability** was initially defined for IT systems or services and only allows for information to be exchanged (see definition below), a more generic definition could be this one:

Interoperability is a property of a product or system, whose [interfaces](#) are completely understood, to work with other products or systems, present or future, without any restricted access or implementation.

This generalized definition can then be used on any system, not only information technology system. It defines several criteria that can be used to discriminate between systems that are "really" inter-operable and systems that are sold as such but are not because they don't respect one of the aforementioned criteria, namely:

- non-disclosure of one or several interfaces
- implementation or access restriction built in the product/system/service

The [IEEE Glossary](#) defines interoperability as:

the ability of two or more systems or components to [exchange information](#) and to use the information that has been exchanged^[1]

What is interoperability?



- Though usually used as a technical term in relation to computers, hardware and software, it is a useful in the context of systems more generally
- Extracting some of the common definitions suitable in the non-computer context:
 - "... the ability of diverse systems and organizations to work together (inter-operate)."
 - "... a property of a product or system, whose interfaces* are completely understood, to work with other products or systems, present or future, without any restricted access or implementation."
 - "... the ability of two or more systems or components to exchange information and to use the information that has been exchanged"

*Interface: (n) "A point where two systems, subjects, organizations, etc., meet and interact."

What is interoperability?



- Though usually used as a technical term in relation to computers, hardware and software, it is a useful term in the context of systems more generally
- Extracting some of the common definitions suitable in the non-computer context:
 - “... the ability of **diverse systems** and organizations to **work together** (inter-operate).”
 - “... a property of a product or system, whose **interfaces* are completely understood**, to work with other products or systems, present or future, without any restricted access or implementation.” “... the ability of two or more systems or components to **exchange information** and to use the information that has been exchanged”
- CPEA seeks to deliver in each of these aspects:
 - Diverse systems working together
 - Promote understanding of points at which systems interact (interfaces) to work with other systems
 - Creating ability to exchange information ... and to use that information

Background to development of CPEA



Timeline



- 2004, 2005 – Adoption of APEC Privacy Framework
- 2007 (June) – OECD Recommendation on Cross-border Cooperation in Enforcement of Laws Protecting Privacy
- 2007 (September) – APEC Data Privacy Pathfinder launched
- 2010 – CPEA established (deliverable of Pathfinder sub-projects 5, 6 and 7)
- 2011 (July) – CPEA commences with 5 participants + Administrator comprising APEC Secretariat and PEAs from Australia NZ and USA
- 2012 – APEC CBPR system ‘built’, CPEA participation a programme requirement for economies’ ‘backstop regulators’
- 2013 (now) – CPEA grown to 22 participants from 8 economies
- 2013+ - review of CPEA scheduled after 3 years of operation

Several stages to get here



- Develop APEC Privacy Framework (2003-05)
 - Starting point OECD Guidelines, many compatible concepts
 - OECD ↔ APEC
 - Clauses 44 and 45 anticipate development of cross-border “cooperative arrangements” in investigation and enforcement
 - Clauses 46-48 anticipate development of CBPRs
- APEC Data Privacy Pathfinder (2007-12): Focus on international implementation (Part IVB of the framework)
 - 8 or 9 sub-projects (5-7 particularly relevant)
 - Principal outcomes:
 - CPEA (2010)
 - CBPR (2012)
- Implementation (domestic, CPEA, CBPR)

Pathfinder subprojects dispute resolution and enforcement



Deliverable	Pathfinder subproject	
CPEA	project 5	contact directories for data protection authorities and privacy contact officers
	project 6	templates for enforcement cooperation arrangements
	project 7	templates for cross-border complaint handling forms
CBPR System requirements	project 8	scope and governance of the CBPR system

Participating Pathfinder economies: Projects 5, 6 and 7 – Australia (leader), Canada, United States, Viet Nam and the ICC participating in projects 5, 6, and 7; New Zealand in projects 6 and 7; Hong Kong China in project 6, and Japan in project 5 and as an observer in projects 6 and 7; Project 8 – Australia (leader), Canada, the ICC.

Projects 5, 6, 7: Combined arrangement



- Decision taken to combine deliverables into a single multilateral MOU or “arrangement” (in preference to other options such as a model bilateral MOU)
- Built upon recently completed OECD Recommendation on Cross-border Enforcement Cooperation – takes a stage further
- Consistent concepts and terminology e.g. “privacy enforcement authority”
- Compatible practical tools (e.g. requests for assistance)

Outcome seeks to promote interoperability:

- Between authorities within APEC region
- Between APEC system and OECD system

Outline of CPEA



CPEA's contents



- Parts 1 – 4, 13, 14: General e.g. objectives, outline, commencement, definitions, costs, disputes
- Part 5: The Administrator
- Part 6: Character of the document [non-binding]
- Part 7: Limitations on Assistance [can decline, prioritisation]
- Part 8: Participation
- Part 9: Cross-border cooperation [detailed machinery, at core is request for assistance]
- Part 10: Confidentiality
- Part 11: Information sharing
- Part 12: Staff exchanges
- Part 15: 3 year review
- Annexes:
 - A: Request for Assistance form
 - B: Contact Point Designation form
 - C: Summary statement of Authority enforcement practices, policies and activities

CPEA's contents Selected highlights for interoperability



- Parts 1 – 4, 13, 14: General e.g. objectives, outline, commencement, **definitions**, costs, disputes
- Part 5: The Administrator
- Part 6: Character of the document [non-binding]
- Part 7: Limitations on Assistance [can decline, prioritisation]
- Part 8: Participation
- Part 9: **Cross-border cooperation** [detailed machinery, at core is request for assistance]
- Part 10: Confidentiality
- Part 11: **Information sharing**
- Part 12: Staff exchanges
- Part 15: 3 year review
- Annexes:
 - A: Request for Assistance form
 - B: **Contact Point Designation form**
 - C: **Summary statement** of Authority enforcement practices, policies and activities

Definitions/concepts clause 4



- Highlight: **Privacy enforcement authority**
- Flexible/broad: encompasses diversity
- Focuses on key common attributes not the areas of domestic difference
- Consistent with OECD Recommendation: anticipates out of region interfaces

'Privacy Enforcement Authority' means any public body that is responsible for enforcing Privacy Law, and that has powers to conduct investigations or pursue enforcement proceedings.

Cross-border cooperation Clause 9.1 – 9.12



Runs through:

- Objective
- Prioritisation
- Also encourage cooperation with non-participants (e.g. CBPR accountability agents)
- Processes preparatory/action/follow through
- Request and response for assistance
- On-going communications
- Use of information obtained
- Notification of breaches/coordination of investigations

Information sharing clause 11



- Interoperability: “ensure interfaces are completely understood”
- Contact point designation – compatible with OECD – since developed combined directory with APEC-COE-OECD
- Participants’ statements of practices, policies and activities in cross-border enforcement: available on each authority’s website and on CPEA website
- Encourage sharing of experience e.g. planned APEC Privacy Enforcement Workshop, Auckland, July 2013



APEC - COUNCIL OF EUROPE - OECD

LIST OF CONTACT POINTS FOR CROSS-BORDER CO-OPERATION
IN THE ENFORCEMENT OF LAWS PROTECTING PRIVACY

This list of contact points has been gathered to facilitate cross-border co-operation in the enforcement of laws protecting privacy by members of APEC, the OECD and the Council of Europe.

The future of CPEA



The future of CPEA



- **CBPR system**
 - CPEA rolled out before CBPR and has a role broader than CBPR enforcement
 - However, from 2013 onwards will see CPEA performing an originally planned supporting role with some new challenges and opportunities
- **Review**
 - Mandated: once CPEA had been operating for 3 years i.e. July 2013 onwards
- **New environment:**
 - E.g. technological and business model changes, developments in global enforcement cooperation alongside or since establishment of CPEA (such as GPEN), exploration of interoperability and enforcement coordination across regions
 - Breach notification: cross-border implications

Any questions?



- Blair Stewart
- Assistant Commissioner (Auckland), Office of the Privacy Commissioner, New Zealand
- Blair.Stewart@privacy.org.nz

- Mark your calendar: **APEC Privacy Enforcement Workshop, Auckland, 16-18 July 2013**