Asia-Pacific
Economic Cooperation

2015/SOM1/ECSG/DPS/006
Agenda Item: 3

APEC Privacy Framework Stocktake: Comparative Review Against 2013 Updates to OECD Guidelines (Narrative)

Purpose: Information
Submitted by: New Zealand

APEC
PHILIPPINES
2015

Data Privacy Sub-Group Meeting
Subic, Philippines
1 February 2015

APEC Privacy Framework Stocktake:

Comparative review against 2013 updates to

OECD Privacy Guidelines

APEC ECSG Privacy Subgroup Meeting

SOM 1, Subic Bay, Philippines, 1 February 2015

Paper prepared by Australia, Canada, New Zealand

APEC Privacy Framework Stocktake: Comparative review against 2013 updates to OECD Privacy Guidelines

This paper provides a comparative review of the APEC Privacy Framework against changes made to the OECD Privacy Guidelines in 2013 and identifies promising directions for updating the APEC Privacy Framework.

Background

In 2013 the DPS decided to undertake APEC Privacy Framework (the 'APEC Framework') to be completed to mark the 10th Anniversary of the Framework due in 2015 (the 'Stocktake').[1] In 2014 the DPS was presented with a proposed Stocktake workplan. It was agreed that the workplan be streamlined to prioritize work elements.

In light of the role of the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (the 'OECD Guidelines') as the foundation and starting point for the APEC Framework, it was agreed that the Stocktake should be based on an understanding and consideration of the 2013 updates to the 1980 OECD Guidelines.[2]

It was therefore decided that one major path to move forward the Stocktake should be a comparative review of the changes to the OECD Guidelines with the APEC Framework, and that proposals for adjustments be developed. Australia, Canada New Zealand agreed to prepare a paper on the subject.

Structure of this paper

The paper provides a comparative review of the 2013 changes to the OECD Guidelines against the APEC Framework in three parts:

- Part A – Outlines principal changes to the OECD Guidelines.
- Part B – Identifies revised OECD Guidelines content that has no counterpart in the APEC Framework.
- Part C – Drawing upon the OECD changes, identifies promising directions to update the APEC Framework[3].

The paper concludes with several findings and recommendations.

[1] See Proposal for Data Privacy Subgroup stock take of APEC Privacy Framework, 2013/SOM1/ECSG/DPS/004.
[2] For a presentation about the 2013 changes to the OECD Guidelines, see: Review of OECD Guidelines, 2014/SOM3/ECSG/DPS/014.
[3] Note that the scope of the Stocktake excludes recommending changes to the APEC information privacy principles themselves. The updates that are in contemplation in this paper relate to such areas as explanatory memoranda, facing page commentary, and the content of Part IV of the Framework (domestic and international implementation).

Part A – Changes to the OECD Guidelines

In 2013, following several years of expert study and wide-ranging review, the OECD adopted a set of changes to the OECD Guidelines. This part of the paper summarises the principal changes.

At the outset, it should be noted that no changes have been made to the 'basic principles of national application' which the OECD Expert Group found to remain appropriate even after 30 years. Those principles are the equivalent to the information privacy principles in the APEC Framework.

Changes have been made to the following:

- definitions,
- implementing accountability,
- basic principles of international application,
- national implementation, and
- international co-operation and interoperability

In addition, the OECD has added a Supplementary Explanatory Memorandum to the Guidelines.

By way of brief elaboration of the changes:

- **Definitions**
  Two new definitions have been added: 'laws protecting privacy' and 'Privacy enforcement authority'. The two definitions are drawn directly from the OECD Recommendation on Cross-border Enforcement in the Enforcement of Laws Protecting Privacy (2007).[4]

- **Implementing accountability**
  A new Part 3 entitled 'implementing accountability' was inserted in the OECD Guidelines. This elaborates the existing accountability principle by reference to privacy management programmes and data security breach notification.

  The new material provides that a data controller should have a privacy management programme and should be prepared to demonstrate to a privacy enforcement authority that its programme is appropriate. The new Part elaborates the necessary elements of a privacy management programme.

  The new Part introduces data security breach notification obligations. Data controllers should give notice to relevant authorities in case of a significant security breach affecting personal data. Further, data controllers should directly notify affected data subjects where those individuals are likely to be adversely affected by the breach.

- **Basic principles of International Application**: **Free flow and legitimate restrictions**
  The 1980 Guidelines contained material on this topic but the text is largely rewritten in the 2013 version. However, not all of the 2013 changes are substantive - the OECD describes the

[4] The definitions are nearly identical to definitions found in the APEC Cross-border Privacy Enforcement Arrangement (CPEA) as the CPEA was drafted to be interoperable with the OECD 2007 Recommendation.

revisions as 'an attempt to simplify and consolidate the OECD approach to transborder flows of personal data'.[5] A few features of the 2013 text that differ from the 1980 version include:

- An explicit opening reference to a data controller's responsibility to be accountable for personal data under its control irrespective of the location of the data.
- A reworking of the text outlining the circumstances where member countries should refrain from restricting transborder flows of personal data. Some of this simply rewords existing material where another country substantially observes the OECD Guidelines. However, the new aspect is reference to sufficient, effective and appropriate measures put in place by a data controller.
- Proportionality and a risk-based approach are made more explicit.

- **National implementation**

  The changes supplement the earlier, and continuing, focus upon the need for laws protecting privacy by elaborating in more detail additional non-regulatory measures. In particular it is stated that state that member countries should:

  - Develop national privacy strategies that reflect a co-ordinated approach across governmental bodies.
  - Establish and maintain privacy enforcement authorities – guidance is given on the attributes and support needed for such authorities.
  - Adopt complementary measures such as education and awareness, skills development, and promoting technical measures which help protect privacy.
  - Consider the role of actors other than data controllers.

- **International co-operation and interoperability**

  The 2013 changes broaden the Part's scope beyond cooperation to include interoperability. Changes include:

  - Explicit reference to the need to enhance information sharing among privacy enforcement authorities.
  - Encouragement of international arrangements to promote interoperability between privacy frameworks.
  - Support for new internationally comparable metrics to inform the privacy policy making process and for openness about observance of the Guidelines.

- **Supplementary Explanatory Memorandum**

  The 2013 changes are accompanied by a Supplementary Explanatory Memorandum (SEM). The SEM runs to 19 closely typed pages with footnotes and covers the context of and process leading to the 2013 update and explains all the principal changes.

[5] See OECD, Supplementary explanatory memorandum on the revised recommendation to the council concerning the guidelines governing the protection of privacy and transborder flows of personal data (2013), 2013.

Part B – Revised OECD Guidelines content that has no counterpart in the APEC Framework

The following highlights those aspects of the 2013 changes to the OECD Guidelines that have no equivalent in the APEC Framework.

- **Definitions**
  The APEC Framework has no definitions that equate to the new OECD definitions of 'laws protecting privacy' and 'Privacy enforcement authority'.

- **Implementing accountability**
  The APEC Framework has no equivalent to the new privacy management programme and data security breach notification features of the 2013 OECD Guidelines.

- **Basic principles of International Application: Free flow and legitimate restrictions**
  Under the APEC accountability principle an information controller is accountable for complying with the principles and should, when transferring information internationally, obtain individual consent or take reasonable steps to protect the information. This provision might be said to have anticipated one of the OECD changes:

New OECD text	Existing APEC text
A data controller remains accountable for personal data under its control without regard to the location of the data.	A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be 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.

  The APEC Framework has no equivalent to the text in the OECD Guidelines (in either the 1980 or 2013 versions) guiding governments generally as to circumstances in which they should refrain from restricting transborder flows of personal data.[6]

  The APEC Framework embeds a risk-based approach at its centre (e.g. the 'Preventing harm principle'). Proportionality may be seen as a feature of that.

- **National implementation**
  The APEC Framework does not include reference to national privacy strategies. However, there is already material in the APEC Framework touching upon several of the other matters covered in the 2013 changes to the OECD Guidelines (e.g. in relation to public education).

[6] Although not equivalent to the OECD approach, it may be noted that APEC Framework discourages unnecessary barriers to cross-border transfers, e.g. paragraphs 30 and 48.

There is no reference in the APEC Framework to the need for privacy enforcement authorities.[7] Nor is there explicit reference to the need to promote technical measures which help protect privacy.

- **International co-operation and interoperability**
  The APEC Framework provides explicit provision for cooperation in investigations and enforcement, which later led to the development to the APEC CPEA. That material is more detailed than anything found in the OECD Guidelines.

  The APEC Framework does not include anything on:
  - Interoperability with privacy frameworks based outside the APEC region.
  - Development of internationally comparable metrics to inform privacy policy making.

- **Supplementary Explanatory Memorandum**
  There is no exact equivalent to the SEM in the APEC Framework. The nearest counterpart is the Framework's preamble and facing page commentary.

[7] The obligation to have a PEA has become a requirement for participation in the CBPRs although that is not explicitly stated in the APEC Framework which preceded the development of the CBPRs.

Part C – Promising directions to update the APEC Framework drawing upon the OECD changes

In evaluating aspects of the 2013 changes to the OECD Guidelines that might usefully be considered for updating the APEC Framework, the following questions might usefully be kept in mind:

- Will the change contribute to the APEC, CTI and ECSG objectives?
- Will the change be in keeping with the general approach of the APEC Framework?
- Will the change help ensure that the APEC Framework more effectively responds to technological and marketplace evolution since 2005?
- Will the change help ensure that the APEC Framework remains 'fit for purpose' for another 10 years?
- Will the change promote interoperability between the APEC Framework and other arrangements at international level?

A. Implementing accountability

The new OECD 'implementing accountability' Part has particular promise given the emphasis that has been given in both the APEC Framework and the ECSG's work in promoting accountability in handling of personal information. The material relates to:

- Privacy management programmes.
- Information security breach notification.

Reference to the concept and elements of a privacy management programme might suitably be incorporated into the APEC Framework Part IVA (Guidance for domestic implementation).

Breach notification might suitably be added into the APEC Framework Part IVA(V) (Guidance for domestic implementation: Providing for appropriate remedies in situations where privacy protections are violated).

The new material may need to utilise the definitions of 'privacy enforcement authority' and 'privacy law' to be borrowed from the CPEA.

It is suggested that including such material in the APEC Framework could bring various advantages:

- Strengthen the existing emphasis of the APEC Framework on accountability and effective redress when things go wrong.
- Breach notification effectively responds to technological and marketplace evolution since 2005 reflected, for instance, in a succession of large data security breaches having cross-border dimension and regional implications.
- Ensure that the APEC Framework remains 'fit for purpose' into the future as privacy management programmes and breach notification are modern, adaptable and flexible approaches.

- Promote interoperability between APEC and OECD arrangements and provide scope for further APEC-OECD cooperation in more detailed work on accountability approaches.

B. Basic principles of International Application: Free flow and legitimate restrictions

The OECD's 1980 approach to transborder data flows was known at the time of the development of the APEC Framework but the ECSG chose not to replicate that approach in the Framework. The 2013 changes are described as 'an attempt to simplify and consolidate the OECD approach'.

It may be timely for APEC to revisit the issue and articulate an approach to the circumstances where restricting cross-border transfers for reasons of privacy are legitimate or not legitimate. The Framework could offer guidance in relation to the public policy considerations in balancing the desirability of uninterrupted cross-border trade and the use of transfer restrictions to protect personal information. Three factors in particular may be noted:

- Since 2005 some APEC economies have imposed restrictions on classes of cross-border transfers by way of general privacy or 'localisation' laws or in laws focusing on special categories of data – and there is little guidance in the APEC Framework in relation to such restrictions.
- The issue continues to arise in the context of free trade agreement negotiations.
- Other international and regional arrangements have settled approaches to the issue of legitimate restrictions on transfers and interoperability may be enhanced if the APEC Framework was explicit on the matter or possibly aligned with the 2013 OECD changes.

Work in this area would seem to support the CTI objectives and priorities in terms of advancing regional economic integration, enhancing regulatory cooperation and advancing regulatory coherence.

It is suggested that including more explicit material in the APEC Framework could bring various advantages:

- Contribute to the APEC objectives of removing distortions that impede trade.
- Promote interoperability between APEC and OECD arrangements and provide scope for further APEC-OECD cooperation in more detailed work on accountability approaches.

C. National implementation

The APEC Framework was a leading document at the time of its adoption for its attention to the non-regulatory measures that usefully supplement the role of privacy laws. The 2013 OECD changes are quite in keeping with the existing APEC approach and would take the Framework in promising directions.

In particular the following are noted:

- The usefulness of national privacy strategies.
- Promotion of technical measures which help protect privacy.
- Explicit reference to privacy enforcement authorities – their role and the attributes and support needed for such authorities.

It is suggested that including such material in the APEC Framework could bring various advantages:

- Strengthen the existing approach of the APEC Framework which already points to several non-regulatory approaches.
- Help ensure that the APEC Framework more effectively responds to technological evolution since 2005 through reference to technical measures (e.g. by promoting Privacy Enhancing Technologies or a privacy-by-design approach).
- Promote interoperability between APEC and OECD arrangements and provide scope for further APEC-OECD cooperation in more detailed work on strategies and promotion of technical measures to protect privacy.

D. International co-operation and interoperability

The APEC Framework might usefully be updated to include promotion of:

- Interoperability with privacy frameworks based outside the APEC region.
- The development of internationally comparable metrics to inform policy making in relation to privacy.

The 2013 OECD changes may suggest a good place to start. APEC has of course already been leading in some areas of privacy interoperability such as:

- APEC: EU mapping exercise in relation to the CBPR/BCR systems.
- Interoperability between the APEC CPEA and the OECD Enforcement Cooperation Recommendation.
- Joint economy/national enforcement contact directory between APEC, OECD and Council of Europe.

Indeed, a recent OECD Roundtable on implementation of the Guidelines featured the APEC-EU work as the best current example of an interoperability initiative.

It is suggested that including such material in the APEC Framework could bring various advantages:

- Contribute to the CTI objectives of enhancing regulatory cooperation and advancing regulatory coherence.
- Support the existing work that the ECSG has been engaged in on interoperability.
- Ensure that the APEC Framework more effectively responds to ongoing technological and marketplace evolution since 2005 by having internationally comparable metrics to inform policy making.
- Promote interoperability between APEC and OECD arrangements and provide scope for further APEC-OECD cooperation in more detailed work on privacy metrics.
- Provide greater authority and direction for DPS work in this area.

E. Supplementary Explanatory Memorandum

A document of the detail and length of the SEM would probably be an unnecessary call on DPS resources. However, it may be worthwhile to contemplate some kind of simply accompanying explanatory material. The SEM may also be useful in some areas for ideas for updating the facing page commentary.

It is suggested that an updated preamble facing page commentary to the principles would be useful given the technological and marketplace evolution since 2005. Aspects of the OECD SEM could be useful for this purpose as will other resources such as the papers presented to DPS workshops.

Findings and recommendations

On behalf of the DPS, and as a contribution to the APEC Privacy Framework Stocktake, Australia, Canada and New Zealand have completed this comparative review of the 2013 changes to the OECD Guidelines with the APEC Framework with a view to making proposals for adjustments to the APEC Privacy Framework.

The recommendation is made below that certain concrete proposals be prepared for updating the APEC Framework. The approach to be taken in any concrete proposals need not be identical to the approach taken by the OECD Guidelines as they must suit APEC conditions and objectives. However, the DPS should give some weight to the benefits of maintaining consistency with the OECD where that enhances interoperability and the facilitation of data transfers beyond the APEC region.

The following findings are offered:

A. The 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were the foundation and starting point for developing the APEC Privacy Framework.
B. The OECD Guidelines and APEC Framework have the same objectives and contain many similarities in terms of structure and content.
C. After 30 years of operation, the OECD Guidelines underwent a major review by experts resulting in the adoption of significant updating changes in 2013.
D. The 2013 changes modernised and supplemented the Guidelines, to make them more effective for the changed technological and business environment, while maintaining the 1980 principles unchanged and basic structure of the Guidelines intact.
E. Given that the origins of the APEC Framework lie in the 1980 version of the OECD Guidelines that are now superseded, and that substantial effort and expertise has gone into updating those Guidelines, it is fitting that the Stocktake should be based on an understanding and consideration of the 2013 updates to the 1980 OECD Guidelines.
F. As a result of the 2013 changes, there are several areas in which the APEC Framework is now lacking counterpart content to the OECD Guidelines.
G. The review has identified several areas where the APEC Framework may benefit from updating in areas where changes have been made to the OECD Guidelines.

Therefore it is recommended that the DPS should study the results of the comparative review and report back to the ECSG at SOM3 with concrete proposals to be considered for updating the APEC Privacy Framework giving particular consideration to the following areas:

a. Incorporation of the concept and elements of a **privacy management programme** into the APEC Framework Part IVA (Guidance for domestic implementation).

b. Adding **breach notification** into the APEC Framework at Part IVA(V) (Guidance for domestic implementation: Providing for appropriate remedies in situations where privacy protections are violated).

c. In Part IVA (Guidance for domestic implementation), include new content promoting:

   i. **Economy privacy strategies**.
   ii. **Technical measures** that will help protect privacy.
   iii. The establishment of **privacy enforcement authorities** with reference to their role and the attributes and support needed for such authorities.

d. In Part IVB (Guidance for international implementation), include text promoting:

   i. **Interoperability** with privacy frameworks based outside the APEC region.
   ii. **Internationally comparable metrics** to inform policy making in relation to privacy.

e. In Part IVB (Guidance for international implementation), in existing part (III) or as a new part (IV), outline the factors to be considered in balancing trade considerations when restricting **cross-border transfers** for reasons of privacy.

f. Make suitable **updates to the preface and facing page commentary**.

19 January 2015