An Overview of the Principles Established by the APEC Privacy Framework

Tony LAM, Acting Privacy Commissioner for Personal Data
Office of the Privacy Commissioner for Personal Data
Hong Kong, China

Introduction

Technological advances have been transformational in developing new business opportunities and devising new ways of doing business. The combined effect brought about by the advent of new technologies, and the move towards a global economy, has been to bring into sharp focus the fact that the protection of data privacy has assumed international proportions.

The concept of data privacy protection is also a natural development in the pursuit of economic growth. The popularity and ubiquitous nature of electronic commerce have created an electronic trading environment in which personal data are freely transferred around the world in vast quantities every second of the day. The question that follows is how to control the flow of personal data across national boundaries in an orderly manner that would not expose the data privacy rights of individuals to undue or unacceptable risks.

In an effort to rationalize the international regulation of data flows, the OECD recommended a set of guidelines on the protection of privacy and trans-border flows of personal data in 1980. The OECD initiative has been further developed by the European Union, which, in 1995, issued a directive on the protection of individuals with regard to the processing of personal data and the free movement of such data.

In the context of electronic commerce development, trans-border dataflow has become an issue that every economy has to deal with sooner rather than later. By definition trans-border traffic will impact upon the regulatory regimes of the exporting and importing economies. There is a need to find a common approach towards data privacy that would not operate as an impediment to the development of cross-border trade. Fulfillment of that need hinges on harmonization.

Regional Co-operation

APEC leaders have recognized that a conducive electronic environment should exist among member economies by addressing common privacy concerns. Ultimately this would have the effect of boosting consumers' trust and confidence in the free flow of information.

The "APEC 1998 Blueprint for Action on Electronic Commerce" laid down the basic ideology shared by member economies and paved the way for future co-operation. APEC Ministers agreed to a "Work Program" to monitor progress by taking into account *"the different stages of development of member economies, the diverse regulatory, social, economic and cultural frameworks in the region"*.

The APEC Senior Officials meeting held in February 1999 in Wellington, New Zealand, approved the establishment of the APEC Electronic Commerce Steering Group (the "ECSG") to ensure continued co-ordination and pursuit for the Blueprint for Action.

In February 2003, the ECSG discussed various approaches towards privacy protection for the region. A principles-based approach agreed by member economies was seen to be both an effective and flexible means that would allow for improvement over time and yet one that would remain technology neutral. The APEC ECSG Data Privacy Subgroup was subsequently formed with the objective of developing a set of APEC Privacy Principles and implementation mechanisms using the OECD Privacy Protection Guidelines as the foundation for discussion.

Eleven member economies are represented on the Privacy Subgroup. They include Australia, Canada, China, Hong Kong, China, Japan, Korea, Malaysia, New Zealand, Chinese Taipei, Thailand and the United States.

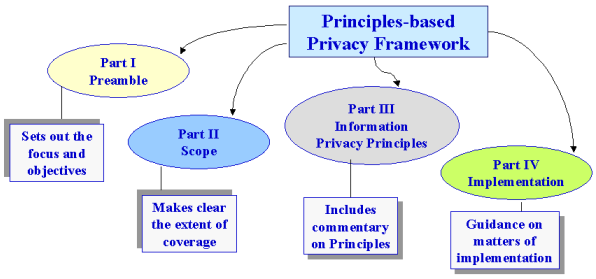
The Privacy Subgroup began its work in 2003 and by September 2004 consensus was reached on a draft set of APEC Privacy Principles. The 2004 APEC Ministerial Joint Statement endorsed the APEC Privacy Framework and the Future Work Agenda on Implementation of the APEC Privacy Framework. APEC Leaders endorsed the Ministerial Joint Statement in full at the 12th APEC Economic Leaders' meeting held in November 2004 at Santiago, Chile.

The APEC Privacy Framework

The Framework seeks to promote a consistent approach to information privacy protection among APEC member economies, while avoiding the creation of unnecessary barriers to information flows. The underlying intent of the Framework, as recognized in its Preamble, is to promote electronic commerce and to ensure the free flow of information within the APEC region. To this end, the Framework has been developed in recognition of the importance of the following points:

- Developing appropriate privacy protection for personal information.
- Recognizing the free flow of information being essential for economies to sustain economic and social growth.
- Enabling global organizations that collect, access, use or process data in APEC economies to develop and implement uniform approaches within their organizations for global access to, and use of, personal information.
- Enabling enforcement agencies to fulfill their mandate to protect information privacy.
- Advancing international mechanisms to promote and enforce information privacy and maintain the continuity of information flows among APEC economies and with their trading partners.

A schematic of the Framework is depicted as follows:

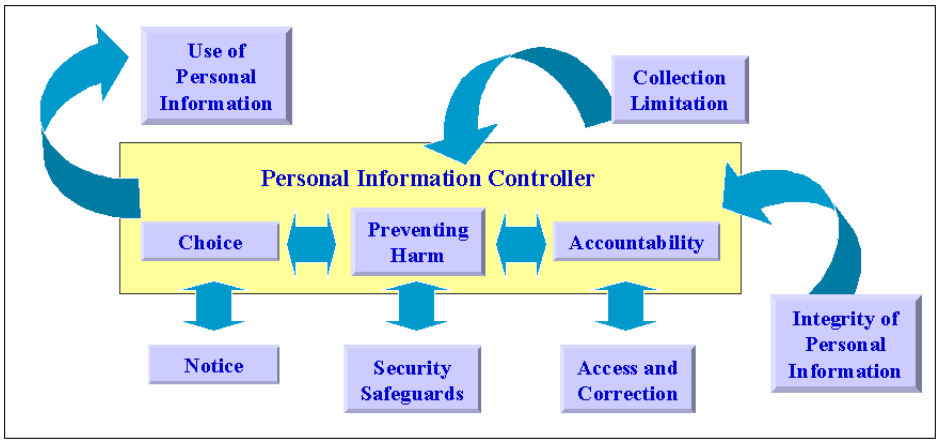


APEC Information Privacy Principles

The Framework's privacy principles and implementation guidance are intended to provide clear directions to businesses in APEC economies regarding common privacy issues, and balancing information privacy with business imperatives. What is also important is that due considerations are given to the cultural, social, economic and other diversities that exist within member economies so that exceptions to the application of the principles might exist.

For example, the Framework recognizes that there are differences in definitions in individual economies on terms such as "personal information" and "personal information controller". It also makes special mention of "publicly available information" which reflects the way such information is treated in certain domestic economies.

Part III of the Framework sets out the provisions of the 9 principles established under the APEC Privacy Framework and their commentary. The following diagram attempts to set out the inter-relationships between the principles on the basis of our understanding of their applications.



.

A Brief Overview of the Principles

I Preventing Harm

This provides that privacy protections be designed to prevent harm to individuals from wrongful collection or misuse of their personal information and that remedies to privacy infringements are proportionate to the likelihood and severity of the risk of harm.

The basic concept of this principle is to anchor APEC privacy protections to alleviating harm to individuals. The prevention of harmful consequences of unwanted intrusion and misuse of personal information is generally recognized as the yardstick in determining the collection, use safekeeping and handling of personal information. The risk of harm is a factor that an information controller should assess when designing data protection measures.

II Notice

This provides for the information a personal information controller must include in the notice to individuals when collecting their personal information and requires that all reasonably practicable steps be taken to provide the notice either before or at the time of collection, otherwise, as soon after as is practicable.

This principle seeks to ensure that individuals understand what information is collected about them and for what purpose it is to be used. Good practice dictates that individuals are informed at the time of, or before, information is collected. In some circumstances it may not be practicable to do so, and when this is the case, the notice should be provided "as soon after as is practicable". This is a requirement tailor-made for e-commerce as very often it is not

practicable for notice to be given on or before collection of data when a prospective customer initiates contact in an online environment.

III Collection Limitation

This provides for the lawful and fair collection of personal information that is relevant to the purposes of collection and where appropriate, with notice to, or consent of, the individual concerned.

This principle limits the collection of information that is relevant to the purposes of collection. In determining what is "relevant", it is intended that "proportionality in relation to the fulfilment of such purposes" may be a determining factor. This concept was introduced as a negotiated substitute for the concept of "adequate but not excessive collection" found in most other privacy frameworks, e.g. Hong Kong, Canada (and other non-APEC jurisdictions such as UK).

IV Use of Personal Information

This limits the use of personal information to fulfilling the purpose of collection and other compatible or related purposes.

The application of this principle requires consideration of the nature of the information, the context of collection and the intended use of the information. A fundamental criterion to determine "compatible or related purpose" is "whether the extended usage stems from or is in furtherance of such purposes".

There are three exceptions to the change of use of personal information. The first is where the individual has given "consent". The second exception is where the individual has initiated the request for a service or product and the third is where the use of personal information is pursuant to legal requirements.

V Choice

This provides, where appropriate, for individuals to be provided with mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information.

Part and parcel of implementing the principle of preventing harm is the need to give the individuals concerned, as far as practicable, an informed choice on or before the collection of their personal information. The emphasis is on a "mechanism" that enables individuals to exercise choice.

For example, a website privacy notification should be crafted in clear language that is "easily understandable" to facilitate rather than obscure understanding. The display of the notice should also be prominent. Though acknowledging that it might not be practicable to give notification in some situations such as where data were not collected directly from individuals or where the data are obtained in a public domain, the right of choice is a principle that should, as far as practicable, be adhered to.

VI Integrity of Personal Information

This provides that personal information be accurate, complete and kept up-to-date to the extent necessary for the purpose of use.

The principle does not adopt the concept of "retention limitation" which is found in most other privacy frameworks although it was once considered. Taking into account technological realities, for example, electronic data cannot be fully destroyed unless physically destroyed, anonymized data can be de-anonymized, it is considered that the retention requirement can be reflected through the requirements of the principle on the use of personal information in which it is required that personal information should not be used when it no longer serves a purpose.

VII Security Safeguards

This requires appropriate security safeguards to be applied to personal information that are proportional to the likelihood and severity of the potential harm, the sensitivity of the information and the context in which it is held.

This principle is premised on the principle of preventing harm. Apart from requiring the security safeguards to be proportional to the likelihood or magnitude of harm, it also requires

a "periodic review and assessment" of the safeguards. This latter requirement can be viewed as consistent with the general regulatory concept of regular privacy compliance audit and evaluation.

VIII Access and Correction

This provides for individuals to have rights of access to their personal information, to challenge the accuracy of the information and, where appropriate, to request correction of such information.

Similar to the provisions of other privacy frameworks, there are exceptions to the access and correction rights of individuals. The first exception is where the burden or expense of complying with the request would be disproportionate to the risks to the individual's privacy in the case. For example, when claims are repetitious or vexatious in nature.

The second exception is where information should not be disclosed because of legal or security reasons or to protect "confidential commercial information". The term "confidential commercial information" is defined and the exception in this case is applied to offer basic protection to trade secrets. This reflects how such information is dealt with in certain jurisdictions. The third exception is where compliance with an access request may result in violating the information privacy of other persons.

IX Accountability

This requires a personal information controller to be accountable for complying with measures that give effect to the Principles. When transferring personal information, reasonable steps should be taken to ensure recipients protect the information in a manner consistent with these Principles.

This principle imposes an obligation on information controllers with respect to the cross-border transfer of personal information. This requires either consent of the individuals concerned or that the data exporter exercise due diligence to ensure recipients protect the information in a manner consistent with the APEC principles.

Concluding Remarks

APEC operates on the basis of non-binding commitments, open dialogue and equal respect for the views of all participants. Decisions made within APEC are reached by consensus and commitments are undertaken on a voluntary basis.

The Hong Kong Privacy Commissioner's Office is pleased to have had the opportunity to work alongside esteemed members of the APEC community during the drafting stage of the APEC Privacy Framework.

Set in a historical context, the APEC Privacy Framework marks an important milestone in the evolution of privacy in that it goes beyond the landmark principles published by the OECD in 1980. Although those principles have stood the test of time, and been robust enough to influence the drafting of privacy legislation in many jurisdictions, they were devised in an era in which desktop PC and E-business were alien concepts. The world has changed immeasurably since then and the APEC Privacy Framework is a reflection of the challenges presented by that change.

In our view, the Framework is a credible instrument that honours cultural diversities and accords due regard to regional differences – an essential ingredient in ensuring broad-based acceptance and lasting utility.