Asia-Pacific
Economic Cooperation

Enabling Electronic Commerce: The Contribution of APEC's Data Privacy Framework

APEC Policy Support Unit
October 2011

Advancing Free Trade for Asia-Pacific **Prosperity**

Prepared by:
Tammy L. Hredzak and Azul Ogazón Gómez
Asia-Pacific Economic Cooperation Policy Support Unit
Asia-Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace, Singapore 119616
Tel: (65) 6891-9600 │ Fax: (65) 6891-9419
Email: psugroup@apec.org │ Website: www.apec.org

Produced for:
Electronic Commerce Steering Group – Data Privacy Sub-Group
Asia-Pacific Economic Cooperation

APEC#211-SE-01.13

The authors would like to thank Akhmad Bayhaqi, Carlos Kuriyama, and Denis Hew of the APEC Policy Support Unit for their helpful comments. We are also grateful to Myung-hee Yoo, Program Director for the APEC Electronic Commerce Steering Group, for her support. The views expressed in this paper are those of the authors and do not necessarily represent those of APEC Member Economies.

CONTENTS

EXECUTIVE SUMMARY

Following the conclusion of APEC's Second Trade Facilitation Action Plan (TFAP II) in 2010, the APEC Policy Support Unit (PSU) conducted the Final Assessment by analysing the contributions made by the working groups in the four priority areas – Customs Procedures, Standards and Conformance, Business Mobility, and Electronic Commerce.

This report has been prepared for the Data Privacy Sub-Group (DPS) of the Electronic Commerce Steering Group (ECSG) to evaluate the impact that the actions of the DPS have made towards improving trade facilitation in the APEC region. APEC's emphasis on trade facilitation has meant that the DPS has been at the forefront of international efforts to improve data privacy, developing the Blueprint for Action on Electronic Commerce, which was endorsed in 1998, and the APEC Privacy Framework, which was endorsed in 2004.

For the TFAP II Final Assessment, 11 APEC economies indicated to the PSU that they have actively considered the APEC Privacy Framework while developing or modifying their domestic data privacy legislation. The number of economies has risen from 2008 when six members reported that they had actively considered or developed domestic privacy frameworks that referred to the APEC Privacy Framework. The actions of the DPS to establish a common approach to data privacy as well as to build capacity in the APEC region are apparent and are producing results.

During the TFAP II period of 2007 through 2010, the DPS developed many valuable initiatives towards improving data privacy in the APEC region. The Data Privacy Pathfinder Initiative is designed to advance the implementation of the APEC Privacy Framework and lead to the development of an APEC Cross-Border Privacy Rules (CBPR) system. There are currently 16 APEC economies participating in the Pathfinder initiative. At the time of its endorsement in 2007, there were 13 APEC members participating in this initiative.

In 2008, the DPS identified and endorsed nine interrelated projects necessary to implement the Pathfinder. The projects were developed to support business needs, reduce compliance costs, provide consumers with effective remedies, allow regulators to operate efficiently, and minimize regulatory burdens. Eight documents, including guidelines, directories and templates, to implement the Pathfinder projects have now been completed by the DPS, thereby creating the framework for the implementation of a CBPR system in the APEC region.

The APEC Cross-Border Privacy Enforcement Arrangement (CPEA), a multilateral arrangement that provides the first mechanism in the APEC region for privacy enforcement authorities to share information and provide assistance, commenced in July 2010. The CPEA signifies the ongoing 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 DPS continues to make great progress building capacity in the APEC region and in implementing projects that establish a common approach to data privacy. By working to improve the privacy of cross-border data flows, the activities of the DPS clearly improve trade facilitation in the APEC region. Additionally, building a foundation of trust and confidence in data networks ensures the growth of electronic commerce in the region, thus

allowing businesses and consumers to reap the benefits associated with electronic commerce, including reduced trade transaction costs.

The DPS should continue to work to ensure that all APEC members become active participants in the Cross-Border Privacy Rules (CBPR) system and in the Cross-Border Privacy Enforcement Arrangement (CPEA). The DPS should also strive to monitor how its achievements improve trade facilitation and reduce trade transaction costs in the APEC region. This could be done by developing quantifiable key performance indicators (KPIs) or through a case study approach that estimates the benefits to the business community as a result of the CBPR system.

1. INTRODUCTION

A. IMPORTANCE OF DATA PRIVACY

The Internet has become a platform for communication, collaboration, innovation, productivity improvement and economic growth, transforming economies and societies in the process. In 2010, there were over 2 billion Internet users in the world, having doubled from the number of Internet users in 2005[1]. In March 2011, there were an estimated 1.2 billion Internet users in the APEC region for a penetration rate of 43% and accounting for 57% of the total number of Internet users in the world[2].

A 2008 study by UNCTAD found that most individuals were using the Internet for the purposes of communicating and obtaining information about goods and services, followed by purchasing or ordering goods or services online[3]. The study also found that a substantial proportion of businesses in many selected APEC economies were placing orders via the Internet, ranging from 7% in Chile to 65% in Canada, while a smaller proportion were receiving orders via the Internet, ranging from 3% in China to 37% in New Zealand.

In recent years, the global economy has witnessed a substantial increase in the volume of e-commerce. This trend shows no signs of slowing down since online transactions make economic activity more efficient, faster, and cheaper. A recent report forecasts that global e-commerce revenue will grow by 19% to USD 680 billion in 2011 and is estimated to reach USD 963 billion by 2013[4]. However, surveys often reveal that customers sometimes refrain from engaging in electronic commerce activities, especially those involving financial transactions, because of concerns over data security and privacy.

Privacy violations can occur when the personal data used to complete an electronic transaction is acquired, stored, sold or used without the awareness or consent of the customer. Head and Yuan identify four parties – privacy subject, collector, illegal user or violator, and privacy protector – that interact in three interrelated activities – information collection, privacy violation, and privacy protection. Given that these parties often have conflicting interests, data privacy can therefore be a complex issue.

Businesses have an incentive to use information technology to identify, collect, and use as much personal information about their customers as possible so that they can better market their products and build more effective business models. Although some customers may appreciate such personalized services, they are also concerned about security and privacy and urge governments to look for ways to increase consumer protection.

Government policies must therefore be oriented to foster transparency and fairness, protecting electronic commerce systems from both internal and external threats, while also protecting consumers and personal information. However, given that information is so easily dispersed globally through electronic transactions, the effectiveness of privacy protection depends on the joint efforts of all parties involved. In addition, differing domestic regulatory

[1] International Telecommunication Union (2010).
[2] Internet World Stats.
[3] UNCTAD (2008).
[4] J. P. Morgan (2011).

frameworks concerning data privacy could lead to a certain level of restriction that negatively impacts trade flows.

The International Telecommunication Union (ITU), the United Nations agency responsible for building confidence and security in the use of information and communications technology (ICT), recognizes that the legal, technical, and institutional challenges posed by data security issues are global and far-reaching, and can only be addressed through a coherent framework of international cooperation that takes into account the role of different stakeholders and existing initiatives. In addition to APEC, there are also other international organizations that seek to foster cooperative efforts in addressing data privacy issues, including the OECD and the European Union.

Global electronic commerce has yet to fully address vital security and privacy issues. A recent series of data breaches involving several high-profile companies and organizations across all industry sectors, ranging from financial institutions to manufacturing firms to government agencies, underscores the continued need for global strategies to improve data security. A survey of over 800 executives at firms around the world found that 27% of companies experienced theft of information during 2010[5].

The survey also found that businesses lost USD 1.7 million per billion in sales due to fraud, a 21% increase over 2009. Annual studies of actual data breaches experienced by companies in the United States since 2005 found that the average organizational cost of a data breach has risen each year, reaching USD 7.2 million in 2010 with an average cost of USD 214 per compromised record[6].

As a result, businesses are increasingly making data security a high priority and are investing more IT spending in this area. Gartner reports that global IT spending is expected to grow by 7% to USD 3.7 trillion in 2011. In addition, ABI Research found that global data security spending rose by 11% to over USD 6 billion in 2010 and forecasts that it will exceed USD 10 billion by 2016. A survey of IT professionals in North America and Europe revealed that data security's share of IT budgets had increased to 14% in 2010 from 8% in 2007[7].

Electronic commerce has the potential to transform the way business is conducted, but its future depends on consumers continuing to increase their level of confidence in conducting business transactions through the Internet and other electronic information systems. Without trust, prudent business operators and consumers may decide to forgo the use of electronic commerce, thus missing out on substantial gains in efficiency. As the OECD states, "absolute trust may never be achievable but users need to be confident that their online activities are as secure as offline equivalents"[8].

B. DATA PRIVACY INITIATIVES IN APEC

APEC has been at the forefront of placing electronic commerce and data privacy issues on the international agenda, having recognized early on the importance of data privacy in fostering trust and confidence within information systems so that information flows for trade could take place without any violation and the benefits of electronic commerce could

[5] Kroll (2010).
[6] Ponemon Institute (2011).
[7] Forrester Research (2011).
[8] OECD (2008a).

therefore be maximized. In 1998, APEC Ministers acknowledged the importance of electronic commerce by endorsing the Blueprint for Action on Electronic Commerce "…to develop and implement technologies and policies, which build trust and confidence in safe, secure and reliable communication, information and delivery systems, and which address issues including privacy, authentication and consumer protection"[9].

The Blueprint sets out the principles for the work of the Electronic Commerce Steering Group (ECSG). The ECSG promotes the development and use of electronic commerce by exploring how APEC economies may best develop legal, regulatory and policy environments that are predictable, transparent and optimized to enable economies across all levels of development to utilize ICT to drive economic growth and social development. Originally established in 1999 as an APEC Senior Official's Special Task Force, the ECSG was aligned to the Committee on Trade and Investment (CTI) in 2007 to enhance the coordination capacity of the ECGS by ensuring a stronger focus on trade and investment issues.

The ECSG is divided into two sub-groups – the Data Privacy Sub-Group (DPS), established in 2003, and the Paperless Trading Sub-Group (PTS), established in 2004. The PTS develops projects on the use of paperless trading in commercial processes involving business-to-business (B2B) and business-to-government (B2G) transactions and promotes the use of electronic documents and Internet technologies in international trade. These projects aim to use "e-solutions" or electronic procedures and processes in cross-border trade to save time and costs for firms and government agencies seeking regulatory compliance information from traders.

The DPS works to establish a common APEC approach to data privacy, developing the APEC Privacy Framework that was endorsed by Ministers in 2004. The APEC Privacy Framework promotes a consistent approach to information privacy protection across APEC economies while avoiding the creation of unnecessary barriers to information flows. The Framework sets out nine Information Privacy Principles, which provide clear guidance and direction to businesses operating in APEC economies: 1) preventing harm; 2) notice; 3) collection limitations; 4) uses of personal information; 5) choice; 6) integrity of personal information; 7) security safeguards; 8) access and correction; and 9) accountability.

The DPS subsequently focused on the domestic and international implementation of the Framework, with a particular emphasis on ensuring that the work of the DPS incorporates capacity building activities for APEC members. To advance the international implementation of the APEC Privacy Framework, Ministers endorsed the APEC Data Privacy Pathfinder Initiative in 2007, which contains general commitments leading to the development of an APEC Cross-Border Privacy Rules (CBPR) system that would enable accountable cross-border data flows under the guidance of the APEC Information Privacy Principles.

The APEC Data Privacy Pathfinder Initiative is designed to support business needs, reduce compliance costs, provide consumers with effective remedies, allow regulators to operate efficiently, and minimize regulatory burdens. The main objectives of the Pathfinder are as follows:

- promote a *conceptual framework of principles* of how cross-border privacy rules should work across APEC economies;

[9] APEC (1998).

- develop and support *consultative processes* between regulators, responsible agencies, lawmaking bodies, industry, third party solution providers, and consumer and privacy representatives;
- produce *practical documents and procedures* that underpin cross-border privacy rules, e.g. self-assessment forms, review criteria, recognition/acceptance procedures, and dispute resolution mechanisms;
- explore ways in which various documents and procedures can be *implemented* in practice; and
- promote *education and outreach* on how an accountable CBPR system works.

The APEC Cross-Border Privacy Rules system would require businesses to develop their own internal rules on privacy procedures governing the movement of personal information across borders. The CBPR scheme would then provide guidance on how these cross-border privacy rules can comply with the APEC Privacy Framework and meet the high standards of the APEC Information Privacy Principles so as to be recognized across APEC economies. The system would thereby build consumer, business and regulator trust in the electronic cross-border flow of personal information across the region.

In 2008, the DPS endorsed a work plan for the Data Privacy Pathfinder, which identified nine interrelated and achievable projects necessary to implement a system of cross-border privacy rules in the APEC region. Four key elements aimed at promoting consumer trust and business confidence in cross-border data flows were identified for the projects and activities developed under the Data Privacy Pathfinder:

- *self-assessment* – organizations use tools and guidance to develop and assess their own internal rules and procedures to protect personal information, thereby making a commitment to be held accountable for compliance with their rules and procedures;
- *compliance review* – the organization's rules are checked by an appropriate external body (e.g., an accountability agent) according to APEC-wide agreed guidelines to ensure that the organization's internal rules and procedures comply with the requirements of the CBPR system;
- *recognition/acceptance* – organizations that have successfully passed the compliance review process will be placed on a list of participating organizations and will be recognized as such in the APEC region; and
- *dispute resolution and enforcement* – domestic and cross-border procedures for resolving complaints, including by appropriate regulators.

The APEC Cross-Border Privacy Enforcement Arrangement (CPEA) is another outcome of the Pathfinder initiative, focusing on the facilitation of both domestic and international efforts to promote and enforce information privacy protections. This multilateral arrangement provides the first mechanism in the APEC region for privacy enforcement authorities to share information and provide assistance for cross-border data privacy enforcement.

Endorsed by APEC Ministers in 2009, the CPEA commenced in July 2010 and currently has five participating economies – Australia; Canada; Hong Kong, China; New Zealand; and the United States. The CPEA signifies the ongoing 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.

2. ASSESSMENT OF THE DPS ACTIONS

A. BACKGROUND

i. APEC's Trade Facilitation Action Plans

APEC has been at the forefront of international efforts to facilitate trade by identifying obstacles that hinder trade and implementing actions and measures to address those obstacles. Based on APEC's Trade Facilitation Principles, the Trade Facilitation Action Plan (TFAP I) was developed in response to the goal set by APEC Leaders in 2001 for member economies to achieve a regional reduction in trade transaction costs by 5% between 2002 and 2006 as progress towards the Bogor Goals.

TFAP I consisted of a menu of actions and measures to reduce trade transaction costs and simplify administrative and procedural requirements in four priority areas – Customs Procedures, Standards and Conformance, Business Mobility, and Electronic Commerce. At the conclusion of TFAP I, APEC members had selected over 1,400 actions and measures in total, of which over 62% had been completed. Based on self-assessments by each economy, APEC Leaders welcomed the achievement of the 5% reduction target in 2006.

Recognizing the benefits of TFAP I to the business community, APEC's Second Trade Facilitation Action Plan (TFAP II) was developed in response to the goal set by APEC Leaders in 2005 to achieve a further reduction of trade transaction costs by 5% between 2007 and 2010. A major component of TFAP II is an updated and revised menu of actions and measures, including some actions that had not been completed under TFAP I, which focus on the same four priority areas and place greater emphasis on Collective Actions and Pathfinders.

TFAP II described 13 actions and measures under two major objectives for the ECSG (see Appendix A for a complete list of the actions):

- *Remove Barriers to Electronic Commerce* – eliminate obstacles for constituents (including citizens, businesses of all sizes, and government agencies) in the global trade flow by identifying, addressing, and alleviating identified barriers and out-of-date practices; and
- *Speed the Use of Electronic Commerce* – build constitute confidence in e-commerce by streamlining processes and removing obstacles.

ii. Development of Key Performance Indicators

In order to measure the impact of their actions and measures on reducing trade transaction costs in the APEC region between 2007 and 2010, each sub-fora developed Key Performance Indicators (KPIs), which were endorsed by the Committee on Trade and Investment (CTI) in 2008. The agreed KPIs for the ECSG are as follows:

Table 1. Endorsed KPIs for Electronic Commerce, 2008

Objective	Action	Output expected	KPI
Implementation of the Data Privacy	Promote the Pathfinder and seek	Full participation and support in the	Number of economies participating in the

Pathfinder	support and participation from economies	Data Privacy Pathfinder by APEC economies	Pathfinder
	Promote the Pathfinder and linkages to domestic data privacy frameworks	Domestic privacy frameworks that refer to the APEC Privacy Framework	Number of economies that actively consider or are developing domestic privacy frameworks that refer to the APEC Privacy Framework
	Implement the various elements of the Pathfinder with regard to cross-border cooperation	Effective cross-border cooperation with respect to the objectives	Number of documents (including guidelines, directories and templates) developed to implement the various Pathfinder projects

Source: APEC (2008).

The TFAP II Interim Assessment conducted in 2009 reviewed these endorsed KPIs. The report noted that the design of KPIs for the actions and measures achieved by the ECSG is especially challenging given the Group's primary focus on the development of a policy framework to facilitate electronic commerce rather than on the implementation of specific reforms that can be quantifiably measured.

In particular, the Data Privacy Pathfinder, a key initiative of the DPS, is inherently unsuited to quantification of the change in trade transaction costs from its adoption. The Pathfinder is not directly aimed at simplification or reduction of trade transaction costs, but rather the facilitation of a cross-border system for the secure transfer of data across the APEC region. Reductions in trade transaction costs may occur indirectly where this generates greater certainty of legal rules governing cross-border data exchange, and only over the longer term. Additionally, generating quantifiable results from the Pathfinder are not feasible until APEC members have addressed data privacy issues domestically and have also established a cross-border system to facilitate data transfer across the APEC region.

Nevertheless, the Interim Assessment suggested three new Key Performance Indicators (KPIs) in order to monitor and evaluate the contribution made by the ECSG members towards the TFAP II goal. These KPIs were recommended as being the most effective, efficient and simple indicators for generating data that are capable of quantifying reductions in cross-border trade transaction costs due to electronic commerce.

Table 2. Recommended KPIs for Electronic Commerce, TFAP II Interim Assessment

Area	Action	Suggested KPI
Remove barriers to electronic commerce	Build government, business and general public confidence in electronic commerce	1. Percentage reduction in operating and service delivery costs
		2. Percentage of relevant data stakeholders can access electronically
		3. Number of stakeholders that have incorporated electronic transactions into their business processes

Source: APEC Policy Support Unit (2009).

The Interim Assessment noted that the recommended KPIs are unlikely to be capable of immediate operation and are also limited in the results that they can generate for the TFAP II period. Additionally, the report did not define the terms used for the KPIs nor specify the data collection methodology. However, agreed interpretations are required in order to measure common transactions and to adequately assess the capacity of members to implement the recommended KPIs.

For the TFAP II Final Assessment conducted by the APEC Policy Support Unit (PSU), the DPS members expressed real difficulty in collecting the data necessary for measurement of the recommended KPIs. Defining the terms used in the KPIs had also proven to be very difficult and agreement on their interpretations had not been reached. The PSU recognizes that the wide-reaching efforts of the DPS and the qualitative nature of its work make measurement of the recommended KPIs extremely difficult.

It is clear, however, that the work of the DPS to establish a common regional approach to data privacy and to promote consumer trust and business confidence in cross-border data flows contributes to improved trade facilitation in the APEC region. Therefore, the DPS Chair suggested that the TFAP II Final Assessment for the DPS be based on the previous KPIs developed by the ECSG and which had been endorsed by the CTI in 2008.

B. ANALYSIS OF KPI 1

Number of economies participating in the Data Privacy Pathfinder

Ministers of 16 APEC economies have endorsed the Data Privacy Pathfinder Initiative – Australia; Canada; Chile; China; Hong Kong, China; Japan; Korea; Mexico; New Zealand; Peru; Philippines; Singapore; Chinese Taipei; Thailand; United States; and Viet Nam.

At the time of its endorsement in September 2007, 13 economies had indicated their participation in the Data Privacy Pathfinder. By July 2008, three additional APEC members had endorsed the initiative (China; Philippines; and Singapore). The participation of additional economies in the Pathfinder illustrates that progress was made during the TFAP II period towards the development of a framework for accountable flows of personal data across the APEC region.

The DPS developed nine projects under the Data Privacy Pathfinder Initiative that are necessary to implement a system of cross-border privacy rules in the APEC region. Given that there is diversity in the levels of development and implementation of domestic privacy frameworks, members selected to participate in those Pathfinder projects that were most appropriate to their economy. Nevertheless, the DPS encouraged all economies to participate in the drafting group for each of the Pathfinder projects – either as an active participant or as an observer – allowing all members to take part in the work from an early stage.

Table 3. Data Privacy Pathfinder Projects

Element	**Project**	
Self-assessment	Project 1	Self-assessment guidance for business
Compliance review	Project 2	Trustmark guidelines for recognition of accountability agents

	Project 3	Compliance review process of CBPRs
Recognition/ acceptance	Project 4	Directories of compliant organizations and consumer contact information
Dispute resolution and enforcement	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
	Project 8	Scope and governance of the CBPR system
	Project 9	Implementation pilot program

Source: APEC (2009).

C. ANALYSIS OF KPI 2

Number of economies that actively consider or are developing domestic privacy frameworks that refer to the APEC Privacy Framework

In July 2008, six APEC economies reported that they were actively considering or developing domestic privacy frameworks that refer to the APEC Privacy Framework, which had been endorsed by Ministers in 2004[10]. For the TFAP II Final Assessment, 11 APEC members indicated to the PSU that they have actively considered the APEC Privacy Framework while developing or modifying their domestic data privacy legislation. This illustrates real progress in developing a consistent approach to information privacy protection across the APEC region through the activities of the DPS over the TFAP II period.

These 11 economies also shared additional information on how they are developing or modifying their domestic data privacy legislation so as to refer to the APEC Privacy Framework. Reflecting the differing levels of development in domestic privacy frameworks, many members are developing or modifying their legislation to incorporate the Information Privacy Principles under the APEC Privacy Framework, while some are looking ahead to the development of the APEC Cross-Border Privacy Rules system and the APEC Cross-Border Privacy Enforcement Arrangement.

The additional inputs the PSU received from each economy have been summarized below (see Appendix B for a complete version of the inputs provided by members).

Australia, a leader for many of the APEC Data Privacy Pathfinder projects, has announced comprehensive reforms to its existing federal law on privacy, the Privacy Act, based on

[10] APEC (2008).

recommendations made by the Australian Law Reform Commission (ALRC). The ALRC referred to the APEC Privacy Framework when considering Australia's current regulation of cross-border data flows of personal information, specifically the concept of accountability as set out in APEC Information Privacy Principle 9, as well as the APEC Data Privacy Pathfinder for the development of a Cross-Border Privacy Rules system. The Government developed an exposure draft of the new privacy principles, which was referred to a Parliamentary Committee for public consultation and report to the Parliament. Following public consultation, the Parliamentary Committee issued its report with recommendations to Parliament in June 2011. The Parliamentary Committee is also considering an exposure draft containing other reforms of the Privacy Act. It is expected that a Privacy Amendment Bill will be introduced and debated in Parliament in 2012.

Canada enacted the Personal Information Protection and Electronic Documents Act (PIPEDA) in 2001. The privacy protections established by this law are consistent with the APEC Privacy Framework and the Principle of Accountability represents a core requirement of the Act. A statutory review of PIPEDA by Canada's Parliament led to the introduction of proposed amendments in May 2010; however, the bill amending the law died on the order paper when the writ was dropped on 26 March 2011. The government is hoping to reintroduce these amendments at the earliest opportunity. Further modifications to the Act were made through Canada's new Anti-Spam Legislation to provide the Privacy Commissioner of Canada with the ability to collaborate with international counterparts in cross-border privacy investigations. These amendments, which enabled the Commissioner to join the APEC Cross-Border Privacy Enforcement Arrangement (CPEA), came into force on 1 April 2011.

Chile is presently working on a draft law that seeks to modify its current privacy legislation (Law 19.628 on Privacy Protection) and which reflects all nine Information Privacy Principles under the APEC Privacy Framework. The bill will soon open for public comment.

Hong Kong, China enacted the Personal Data (Privacy) Ordinance (PDPO) in 1995, in which the data privacy principles are generally in-line with the Information Privacy Principles under the APEC Privacy Framework. In addition, the development of the APEC Data Privacy Pathfinder projects, particularly the APEC Cross-Border Privacy Enforcement Arrangement (CPEA), is seen as a means to enhance its personal data privacy protection and enforcement efforts.

Korea is currently developing a domestic privacy framework that refers to the APEC Privacy Framework and has recently legislated the Privacy and Data Protection Law in March 2011. This legislation implicitly references three Information Privacy Principles under the APEC Privacy Framework: security safeguards, access and correction, and accountability.

Mexico enacted the Federal Law on the Protection of Personal Data Held by Private Parties (LFPDPPP) in July 2010, aligning data privacy protection standards in Mexico with those internationally. This legislation lists eight privacy principles, which refer to the following seven Information Privacy Principles under the APEC Privacy Framework: preventing harm, notice, collection limitations, uses of personal information, choice, integrity of personal information, and accountability.

The **New Zealand** Law Commission completed a major review of the Privacy Act 1993 in July 2011 and made over 100 recommendations. The report specifically references the APEC

Privacy Framework; in particular, the report recommended that the current Privacy Act be amended to allow for future adoption of a regional cross-border privacy rules system (i.e., the APEC Cross-Border Privacy Rules system).

Peru recently developed a legal framework for the protection of data privacy in addition to it being a constitutional right. The Law on the Protection of Personal Data was adopted in July 2011 and is partially based on the APEC Privacy Framework. In developing its domestic data privacy legislation, Peru used the information shared through the APEC workshops and seminars related to the establishment of a policy framework for data privacy. Peru expects that the technical assistance provided through the capacity building efforts of the DPS will be especially relevant for the implementation of its domestic data privacy system.

The Philippines is currently developing its domestic data privacy framework so that it is aligned with the APEC Privacy Framework. The data privacy bill has passed in the House of Representatives and deliberations have started in the Senate. Although there is still no comprehensive data privacy law in the Philippines, the Department of Trade and Industry (DTI) issued Department Administrative Order No. 8 "Prescribing the Guidelines for the Protection of Personal Information in ICT Systems in the Private Sector" in 2006.

Singapore is currently developing data protection legislation, which is intended to be introduced for Parliament's consideration in 2012. This legislation has been drafted taking into consideration international best practices in data protection, including the APEC Privacy Framework. Singapore is also closely following the development of the APEC Cross-Border Privacy Enforcement Arrangement (CPEA), which it believes will provide useful guidance on the treatment and collaboration for cross-border data privacy enforcement.

The United States Department of Commerce recently issued a report detailing initial policy recommendations aimed at promoting consumer privacy online. The report calls for the adoption of a comprehensive baseline set of data privacy standards, based on the Fair Information Practice Principles (FIPPs), which were the basis for the OECD Guidelines and the APEC Privacy Framework. The report also emphasizes the importance of global privacy policy interoperability based on accountability. The APEC Cross-Border Privacy Rules system is specifically referenced as advancing this concept because it incorporates specified accountability requirements for participating businesses and provides for effective protection for consumers. The report also specifically recommends that the United States continue to support the APEC Data Privacy Pathfinder projects as a model for the kinds of principles that can be adopted by groups of economies with diverging legal data privacy frameworks.

D. ANALYSIS OF KPI 3

Number of documents (including guidelines, directories and templates) developed to implement the various Data Privacy Pathfinder projects

Since the Data Privacy Pathfinder Initiative had only just been endorsed by Ministers in 2007, there were no documents developed at the start of the TFAP II period to implement the Pathfinder projects. However, during the TFAP II period, the DPS developed documents to implement each of the four elements of the CBPR system: self-assessment, compliance review, recognition/acceptance, and dispute resolution and enforcement.

Table 4. Documents to Implement the Data Privacy Pathfinder Projects

Element	Document		Completion date
Self-assessment	Project 1 – Self-assessment Questionnaire for Business (2010/SOM3/CTI/021a)	The purpose of this document is to assist organizations in developing and assessing their own internal rules and procedures to protect personal information	2010
Compliance review	Project 2 – Accountability Agent Recognition Criteria	This document sets out the criteria necessary for an Accountability Agent to participate in the APEC Cross-Border Privacy Rules (CBPR) system	2010
	Project 3 – Cross-Border Privacy Rules (CBPR) Compliance Assessment Guidelines for use by Accountability Agents	The purpose of these guidelines is to assist recognized Accountability Agents as they undertake the APEC CBPR compliance review process in a consistent manner across participating APEC economies	2011
Recognition/ Acceptance	Project 4 – Directories of Compliant Organisations		2011
Dispute resolution and enforcement	Project 5 – Request for Contact Point Information with Explanatory Material	This series of documents resulted in the APEC Cross-Border Privacy Enforcement Arrangement (CPEA) commencing operation on 16 July 2010 with five participating APEC members	2009
	Project 6 – APEC Cooperation Arrangement for Cross-Border Privacy Enforcement		
	Project 7 – Request for Assistance Form		
	Project 8 – Guidelines and Procedures for Responsive Regulation in CBPR Systems		2011

Source: Provided by the ECSG-DPS Chair.

By the end of the TFAP II period in 2010, eight documents had been developed to implement the Pathfinder projects – five had been completed, while three were still in progress. The DPS completed the final three documents in 2011, thereby creating the framework for the implementation of a Cross-Border Privacy Rules system in the APEC region.

E. EVALUATION OF THE KPIS

The KPIs used in the Final Assessment, which had been endorsed in 2008, are not entirely effective for measuring the direct output from the actions and measures of the DPS towards the TFAP II goal. Additionally, for the specific actions of the DPS, they do not provide a

quantitative benchmark against which progress can be assessed, nor a methodology for analyzing comparable data over time. However, these KPIs do allow for a qualitative inference of the progress that has been made through the actions of the DPS, especially in the area of trade facilitation, and are more helpful in this purpose compared with the KPIs that had been suggested during the Interim Assessment.

Although the KPIs require very few resources to implement, given their lack of effectiveness, they are not efficient indicators to evaluate the reduction in trade transaction costs made through the actions of the DPS. Since there is no direct link between the KPIs and the actions and measures of the DPS towards the TFAP II goal, there is also no way to measure the costs incurred in achieving those specific actions and measures.

In general, the three KPIs are simple and easy to measure. However, the interpretation and use of the KPIs to measure the actions of the DPS towards improving trade facilitation requires prior knowledge of APEC's work on data privacy. Additionally, the KPIs do not allow for a quantitative analysis of how the actions of the DPS directly contribute to changes in the level of trade transaction costs or improvements in trade facilitation. Therefore, the ability of the KPIs to lead to an understanding of the extent to which the actions of the DPS have reduced trade transaction costs in the APEC region is limited.

Given that the KPIs used in the Final Assessment were not devised for the express purpose of measuring the impact on trade transaction costs, the DPS should endeavor to devise KPIs that can quantitatively measure the progress made through its specific actions and measures under TFAP II. These quantitative KPIs should therefore produce results that can meet the criteria of effectiveness, efficiency and simplicity.

3. CONCLUSION AND RECOMMENDATIONS

A. CONCLUSION

The work of the DPS has put APEC at the forefront of placing electronic commerce and data privacy issues on the international agenda. Much progress has been made through the efforts of the DPS towards a consistent approach to information privacy protection across the APEC region while avoiding the creation of unnecessary barriers to information flows. The DPS has spearheaded several initiatives to implement the APEC Privacy Framework, including the APEC Cross-Border Privacy Rules (CBPR) system and the APEC Cross-Border Privacy Enforcement Arrangement (CPEA).

By the end of the TFAP II period in 2010, 16 APEC members had endorsed the Data Privacy Pathfinder Initiative and eight documents had been developed to implement the Pathfinder projects. In addition, 11 APEC members indicated that they have actively considered the APEC Privacy Framework while developing or modifying their domestic data privacy legislation. These findings reveal the progress that has been made by the DPS towards developing a consistent approach to information privacy protection across the APEC region.

There is a sense of real progress as the DPS moves forward in implementing the APEC Privacy Framework through the APEC Cross-Border Privacy Rules (CBPR) system and the APEC Cross-Border Privacy Enforcement Arrangement (CPEA), in which more focus is given to cross-border flows of data and information sharing. Through the CBPR system and the CPEA, the DPS continues to work to develop an international approach to a consistent and secure data privacy framework across the APEC region.

B. RECOMMENDATIONS

To ensure that businesses and consumers across the APEC region reap the full benefits associated with a secure data network, including increased electronic commerce activities, the DPS should strive to ensure that all member economies become active participants in the Cross-Border Privacy Rules (CBPR) system and in the Cross-Border Privacy Enforcement Arrangement (CPEA). Capacity building efforts among the APEC members should also continue so that more economies are able to develop and modify their domestic data privacy legislation with reference to the Information Privacy Principles under the APEC Privacy Framework.

Given that the adjustment of domestic data privacy regulations towards convergence and harmonization in a regional framework has its own specific challenges, APEC members should also continue to exchange information related to their progress in terms of domestic data privacy regulations. This approach will help to avoid any inconsistencies that may otherwise occur between domestic data privacy regulations and regional frameworks as they develop over time. The APEC CBPR system and the CEPA are clearly steps in the right direction and should be supported by all APEC members.

The DPS should also strive to monitor how its achievements improve trade facilitation and reduce trade transaction costs in the APEC region, especially through the implementation of the APEC Privacy Framework. Since the actions of the DPS can be expected to indirectly

reduce trade transaction costs over the longer term, the DPS should develop quantifiable KPIs that could measure and assess its contributions, enabling the DPS to fully evaluate the achievements made by APEC members in the area of data privacy. For example, the DPS could work towards agreement of the definitions of the terms used in the KPIs that were recommended during the TFAP II Interim Assessment.

Alternatively, a case study approach could be used to evaluate the impact of the DPS initiatives on improving trade facilitation and reducing trade transaction costs in the APEC region. A possible example could be a case study to estimate the benefits that have accrued to the private sector through increased electronic commerce as a result of a more secure data privacy environment due to the implementation of the APEC Cross-Border Privacy Rules system.

Finally, given the global nature of personal information flows, the DPS should also continue its collaborative efforts with other international organizations working in this area, including the OECD and the ITU, particularly in the areas of knowledge sharing and capacity building. These mutual efforts to improve trust and confidence in the protection of personal information will ensure that international frameworks to protect data privacy are robust and secure, thereby enabling electronic commerce and its associated benefits to flourish across the APEC region.

REFERENCES

ABI Research (2011), "World Enterprise Network and Data Security Markets", 10 January 2011.

Antón, A. I. and J. B. Earp (2000), "Strategies for Developing Policies and Requirements for Secure Electronic Commerce Systems", 1st Workshop on Security and Privacy in E-Commerce at CCS2000.

APEC (1998), "APEC Blueprint for Action on Electronic Commerce".

APEC (2005), "APEC Privacy Framework", APEC Secretariat.

APEC (2008), "Committee on Trade and Investment Annual Report to Ministers", APEC Secretariat.

APEC (2009), "APEC Data Privacy Pathfinder Projects Implementation Work Plan – Revised", First Technical Assistance Seminar on the Implementation of the APEC Data Privacy Pathfinder, 2009/SOM1/ECSG/SEM/027, 22-23 February 2009.

APEC (2010), "APEC Fact Sheet: APEC Cross-border Privacy Enforcement Arrangement", July 2010.

APEC Policy Support Unit (2009), "Reducing Trade Transaction Costs in APEC Economies by 5% – Progress with Achieving the Goals of TFAPII".

Busch, A. (2010), "The Regulation of Privacy", Jerusalem Papers in Regulation & Governance, Working Paper No. 26, September 2010.

Forrester Research (J. Penn, H. Shey, et. al.), "Forrsights: The Evolution of IT Security, 2010 to 2011", 15 February 2011.

Gartner (R. Gordon), "Forecast Alert: IT Spending, Worldwide, 2008-2015, 2Q11 Update", ID Number: G00214540, 28 June 2011.

Head, M. and Y. Yuan (2001), "Privacy Protection in Electronic Commerce: A Theoretical Framework", Human Systems Management, 20, pp. 149-160.

International Telecommunication Union (2010), "The World in 2010", 20 October 2010, available at http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf.

Internet World Stats, available at http://www.internetworldstats.com/stats.htm, accessed 1 August 2011.

J. P. Morgan (2011), "Nothing But Net: 2011 Internet Investment Guide", 3 January 2011.

Kroll (2010), "Global Fraud Report: Annual Edition 2010/11".

Marchany, R. C. and J. G. Tront (2002), "E-Commerce Security Issues", Proceedings of the 35th Annual Hawaii International Conference on System Sciences.

OECD (2008a), "The Future of the Internet Economy", Policy Brief, June 2008, available at http://www.oecd.org/dataoecd/20/41/40789235.pdf.

OECD (2008b), "Shaping Policies for the Future of the Internet Economy", OECD Ministerial Meeting on the Future of the Internet Economy, 17-18 June 2008, available at http://www.oecd.org/dataoecd/1/29/40821707.pdf.

Ponemon Institute (2011), "2010 Annual Study: U.S. Cost of a Data Breach", March 2011.

Rule, J. B. and G. Greenleaf (2008), "Global Privacy Protection: The First Generation", Edward Elgar Publishing.

Udo, G. J. (2001), "Privacy and Security Concerns as Major Barriers for E-Commerce: a Survey Study", Information Management & Computer Security, 9/4, pp. 165-174.

UNCTAD (2004), "E-Commerce and Development Report 2004", available at http://www.unctad.org/en/docs/ecdr2004_en.pdf.

UNCTAD (2008), "The Global Information Society: a Statistical View", April 2008, available at http://www.unctad.org/en/docs/LCW190_en.pdf.

APPENDIX

A. TFAP II ACTIONS AND MEASURES FOR ELECTRONIC COMMERCE

1. Remove Barriers to Electronic Commerce

Objective

To eliminate obstacles for constituents (including citizens, businesses of all sizes and government agencies) in the global trade flow by identifying, addressing and alleviating identified barriers and out-of-date practices.

Actions

a) Identify and map out major barriers to e-commerce through the exchange of practices, including but not limited to laws, regulations and policies, on e-commerce across APEC.

b) Ensure compatibility among government, business and the community in online interactions including providing for authentication, confidentiality and certainty in online interactions.

c) In consultation with the private sector, develop a Web portal that will allow all data collected as part of the exchange of practices on e-commerce to be entered directly via the Internet. In addition to streamlining responses and data gathering, the data will be more easily extracted to create an external (unrestricted) site that economy constituents can reference regarding current trade practices on general concepts as well as export-related forms and financing assistance.

d) Continue work in APEC TEL on developing regulatory frameworks that facilitate the convergence of telecommunications, information technology and broadcasting.

2. Speed the Use of Electronic Commerce

Objective

To build constituent confidence in e-commerce by streamlining processes and removing obstacles.

Actions

a) Facilitate the use of secure electronic payment methods.

b) Promote consumer and business education on legal issues.

c) Implement policies that result in the competitive supply of information and communication services.

d) Reduce business costs through increased transparency.

e) Assist the private sector with their network security and data privacy efforts and explain the economic reasons behind developing sound network security and data privacy practices.

f) Develop an e-government portal for procurement that will produce improved and faster information flows, more informed and predictable supply chain and logistics from better requirements tracking, and increased potential for improved oversight and visibility of suppliers and bidding processes.

g) Increase trust and confidence in electronic transactions and e-commerce to counter problems associated with a lack of effective authentication.

h) Facilitate e-commerce adoption in industries, particularly SMEs, to address industry-specific obstacles in e-commerce.

i) Encourage member economies to share information on IT security incidents and collaboratively promote IT security awareness among governments, businesses and the general public.

B. INFORMATION FOR KPI 2 SUBMITTED BY APEC MEMBERS

Economy	Does your economy consider or is your economy developing domestic privacy frameworks that refer to the APEC Privacy Framework (in particular, during the TFAP II period, 2007-2010)?	Provide how the APEC Privacy Framework (e.g., domestic legislation or guidelines, etc.) is referred to or any other information that can show the impact of the policy work of the DPS on the development/improvement of the data privacy system in your economy.
Australia	Yes: Australia is developing a domestic privacy framework that refers to the APEC Privacy Framework.	The Australian Government has announced comprehensive reforms for Australia's existing federal law on privacy, the Privacy Act. The Government's reforms are based on the recommendations made in a report of the Australian Law Reform Commission (ALRC). The ALRC undertook a comprehensive review of privacy law in Australia. When considering Australia's current regulation of cross-border data flows of personal information, the ALRC specifically referred to the APEC Data Privacy Framework. The ALRC focused on the concept of accountability as set out in APEC Privacy Principle 9, as well as the APEC Data Privacy Pathfinder for the development of a Cross-Border Privacy Rules system. The Government has subsequently released exposure draft legislation implementing the Government's response to the ALRC recommendations to a Parliamentary Committee for public consultation and report. The exposure draft legislation contained Australian Privacy Principle 8 (APP 8) on the cross-border disclosure of personal information. After public consultation and considering submissions, the Parliamentary Committee issued its report to Parliament in June 2011. The Parliamentary Committee made a number of recommendations intended to improve guidance and public understanding of the proposed operation the new APP 8. The Government will consider the Parliamentary Committee's recommendations in developing a draft Privacy Bill for introduction into the Parliament. It is expected that the Privacy Bill will be debated in Parliament in early 2012.
Canada	Yes	Canada enacted the *Personal Information Protection and Electronic Documents Act* (PIPEDA) in 2001. The privacy protections established by this law are consistent with the APEC Privacy Framework, the Principle of Accountability representing a core requirement of the Act. A statutory review of this law by Canada's Parliament led to the introduction of proposed amendments in May 2010, however the bill amending PIPEDA died on the order paper when the writ was dropped on March 26, 2011. The government is hoping to reintroduce these amendments at the earliest opportunity. Further modifications to the Act were made through Canada's new Anti-Spam Legislation to provide the Privacy Commissioner of Canada with the ability to collaborate with her international counterparts in cross-border privacy investigations. These amendments, which enabled the Commissioner to join the APEC Cross-Border Privacy Arrangement (CPEA), came into force on April 1, 2011.
Chile	Yes. Chile is currently working on a draft law (bill) which seeks to modify current	Chile recognizes the importance of protecting information privacy to facilitate effective communication and information flow between economies, and to build consumer confidence and security to enable electronic

Economy	Does your economy consider or is your economy developing domestic privacy frameworks that refer to the APEC Privacy Framework (in particular, during the TFAP II period, 2007-2010)?	Provide how the APEC Privacy Framework (e.g., domestic legislation or guidelines, etc.) is referred to or any other information that can show the impact of the policy work of the DPS on the development/improvement of the data privacy system in your economy.
	privacy legislation. The bill will soon open for public comment and if approved will modify Law 19.628 on Privacy Protection (http://www.leychile.cl/N?i=141599&f=2010-10-25&p=) It must be noted that the comments herein apply to the current draft. A process of consultancy and approval are pending and required before becoming effective legislation. Translations used in this report are unofficial.	commerce. The current draft law implicitly reflects the APEC Privacy Guidelines as outlined below. <u>Definitions</u> The bill introduces the term "definitions" to Law 19.628 to clarify terms. ▪ Personal information – current law refers to information refers to any information about "indentified or identifiable" individuals; modification (Article 2, f.) broadens the definition to include "legal persons". ▪ Personal information controller – Article 2, q. creates the definition of personal information controllers. They are defined as "natural or legal persons, public authority, service or any entity that, individually or with third parties, control partly o entirely the treatment of a database or entry of personal information on behalf of a responsible third party." The entity responsible for data is defined in current Law 19.628 under Article 2, n. <u>Principles</u> ▪ Preventing harm – reflecting APEC privacy principle I,14; modifications to proportionality and security include: o Article 3,a: Principle of proportionality – whereby data must be adequate, pertinent and not excessive in relation to their stated and legitimate collection purpose o Article 3,d: Principle of limitation of use – whereby data use will be limited to those purposes defined during collection o Article 3,e: Principle of data security – whereby those responsible for data processing will employ adequate technical and organizational security to prevent unauthorized access, loss, destruction, use or modification. ▪ Notice - reflecting APEC privacy principle II,15; modifications to proportionality and security include: o Article 3,c: Principle of specification of purpose – whereby the purpose of the data collection must be stated, at latest, at the time of collection o Article 3, g: Principle of transparency – whereby the titleholder of information must be informed of collection purpose and transfers to third parties both domestic and international. o Article 4 – considers consent and established when this must be explicit, and when this is revoked.

Economy	Does your economy consider or is your economy developing domestic privacy frameworks that refer to the APEC Privacy Framework (in particular, during the TFAP II period, 2007-2010)?	Provide how the APEC Privacy Framework (e.g., domestic legislation or guidelines, etc.) is referred to or any other information that can show the impact of the policy work of the DPS on the development/improvement of the data privacy system in your economy.
		▪ Exceptions (APEC principle II, 17) – exceptions are expressed in Article 4, (2°) and include: o where the data is from an unrestricted public source o where the data is used by a public institution in its functions as expressly permitted by law o where the data is transferred between public institutions for the purpose of service provision to the titleholder o where the data is required for official statistics o where data is used in the case of health emergency ▪ Collection limitation – reflecting APEC privacy principle III: as detailed above the following articles deal with limitation and proportionality. o Article 3,d: Principle of limitation of use – whereby data use will be limited to those purposes defined during collection o Article 3,a: Principle of proportionality – whereby data must be adequate, pertinent and not excessive in relation to their stated and legitimate collection purpose ▪ Uses of personal information. Relevant text dealing with APEC privacy principle IV is dealt with above as specified in proposed Articles 3,c. and Articles 4 and 4 (2°). ▪ Choice, access and correction – reflecting APEC privacy principles V and VIII: In addition to the above reference to Article 3, f. regarding the principle of access, correction and opposition, proposed Article 4 (3°) entitled "Deber de información y sus contenidos" stipulates the obligation to inform the titleholder of: o the existence of a registry or database to in which personal information may be kept, and the purpose(s) for the same o the consequences of having personal data kept in the database or registry o rights to access, correction, dispute, and cancelation of data o right to revocation of authorization for the management of the titleholder's personal information o the circumstances under which this data may become public In addition Article 14 entitled "Derechos de oposición, rectificación, cancelación y bloqueo del titular" stipulated the titleholder's right to demand modification of his/her personal information under the following circumstances:

Economy	Does your economy consider or is your economy developing domestic privacy frameworks that refer to the APEC Privacy Framework (in particular, during the TFAP II period, 2007-2010)?	Provide how the APEC Privacy Framework (e.g., domestic legislation or guidelines, etc.) is referred to or any other information that can show the impact of the policy work of the DPS on the development/improvement of the data privacy system in your economy.
		○ the responsible entity lacks legal fundament for the management of such information ○ the information has expired ○ the titleholder is deceased (in this case the titleholder heirs have this right) ○ the titleholder has revoked permission for the administration of his/her personal information ○ the information is used for commercial purposes for which the titleholder does not wish to participate Exceptions to these rights (per APEC privacy principle VIII, 25.) are expressed in proposed Article 15. Furthermore Article 9 requires the responsible entity of a registry or database to maintain a permanent website link whereby the public are able to inform themselves of the databases administered by the entity. ▪ Integrity of personal information – reflecting APEC privacy principle VI: the principle of quality as proposed in Article 3, b. requires personal data to be accurate, complete and current in relation to the purpose of its collection. ▪ Security safeguards – reflecting APEC privacy principle VII, 22: as previously stated, Article 3, 3. of the proposed legislation is the principle of data security whereby those responsible for data processing must employ adequate technical and organizational security to prevent unauthorized access, loss, destruction, use or modification. <u>Accountability</u> The APEC privacy framework requires through its principle of accountability, appropriate measures that give effect to the previous stated principles. To this end the draft law sets out the following: ▪ Infringement (Article 23) – conditions for infringement are defined and classified by severity: ○ minor ○ serious ○ very serious ▪ Sanctions (Article 24) which are levied on the above categorization of infringement severity ▪ Framework potential for the participation in the APEC Cross-border Privacy Enforcement Arrangement (CPEA) via the following mechanisms: ○ Model of infringement – which may be adopted by organizations and which involves the designation of a party responsible for prevention, related duty specification including certification

Economy	Does your economy consider or is your economy developing domestic privacy frameworks that refer to the APEC Privacy Framework (in particular, during the TFAP II period, 2007-2010)?	Provide how the APEC Privacy Framework (e.g., domestic legislation or guidelines, etc.) is referred to or any other information that can show the impact of the policy work of the DPS on the development/improvement of the data privacy system in your economy.
		o Compliance certification agencies – overseen by the National consumer Service (SERNAC) and charged with certifying compliance of the Infringement Model of third party organizations through external audit. Should these agencies be deemed homologous and compliant with the Accountability Agencies per the APEC Data Privacy Pathfinder, the draft law may set the framework for participation in the CPEA. This brief is intended to highlight the policy work of Chile in data privacy with regard to the ECSG Data Privacy Subgroup participation.
Hong Kong, China	Yes.	The Personal Data (Privacy) Ordinance ("PDPO") in Hong Kong was enacted in 1995. The Data Privacy Principles under our Ordinance are generally in-line with the APEC Information Privacy Principles outlined in the APEC Privacy Framework. Details can be found in the Information Privacy Individual Action Plan of Hong Kong China. The biannual meetings of the DPS enable us to keep up-to-date about the latest privacy initiatives of various APEC member economies. The development of the APEC Data Privacy Pathfinder Projects, in particular the APEC Cross-Border Privacy Enforcement Arrangement ("CPEA"), would enhance our personal data privacy protection and enforcement efforts by facilitating cross-border information sharing and assistance in enforcement cases involving cross-border data transfer. The Office of the Privacy Commissioner for Personal Data of Hong Kong China has joined the CPEA.
Korea	Yes: Korea considered and is developing a domestic privacy framework that refers to the APEC Privacy Framework	**① Domestic Privacy Framework** - South Korea has Privacy framework based on Act on Promotion of Information and Communication Network Utilization and Information Protection, etc.(1999) and Act on the Protection of Personal Information and maintained by Public institution(1994) - Recently, South Korea legislated Privacy and Data Protection Law(2011.3) to improve privacy framework in public and private sectors. ※ "Personal Information" is that the information pertaining to an individual alive, which contains information identifying a specific person with a name, a national identification number, or similar in a form

Economy	Does your economy consider or is your economy developing domestic privacy frameworks that refer to the APEC Privacy Framework (in particular, during the TFAP II period, 2007-2010)?	Provide how the APEC Privacy Framework (e.g., domestic legislation or guidelines, etc.) is referred to or any other information that can show the impact of the policy work of the DPS on the development/improvement of the data privacy system in your economy.
		of code, letter, voice, sound, image, or any other form(including information that does not, by itself, make it possible to identify a specific personal but that enables to identify such personal easily if combined with another information) **② Assessment Questions Added for Assessment Criteria for Compliance with Requirements of APEC privacy Principle** 1. Do you collect to minimized personal information by Collection Limitation Principle in OECD Guideline? 38. Do you notice the collect and delete personal information of Personal information agent? 45. Do you operate the Personal Information Protection Center against invasion and misuse of personal information? **③ Korea's case to reflect Privacy Framework(Privacy and Data Protection Law)** - security safeguards : Information processor has to safely manage personal information considered possibility to invade the right of information agent(Example Privacy Impact Assessment for analyzing risk factors of information systems and assessing the improvement of IS) - Assess and amendment : Secure the right of inspection and correction(correction, delete, etc.) for information agents and disclosure to process, transmitting and receive the personal information - Accountability : Information processor obey and practice Privacy and Data Protection Law focused on the effort to get confidence of information agent
Mexico	Yes	On **July 6, 2010** came into force the Federal Law on the Protection of Personal Data held by individuals (LFPDPPP). This legislation allows Mexico to align with the standards in the protection of personal data available internationally. The Act is of public order and general observance throughout the Republic and aims at the protection of personal data held by individuals, in order to regulate the legitimate treatment, monitoring and reporting, in order to ensure privacy and the right to informational self-determination of people. In the article 6, it refers that "those responsible for the processing of personal data shall observe this principles".

<table>
<tr><th>Economy</th><th>Does your economy consider or is your economy developing domestic privacy frameworks that refer to the APEC Privacy Framework (in particular, during the TFAP II period, 2007-2010)?</th><th>Provide how the APEC Privacy Framework (e.g., domestic legislation or guidelines, etc.) is referred to or any other information that can show the impact of the policy work of the DPS on the development/improvement of the data privacy system in your economy.</th></tr>
<tr><td></td><td></td><td>

Legality
Consent
Information
Quality
Purpose
Loyalty
Proportionality
Accountability

This principles listed previously, refer to the APEC Privacy Framework:
<table>
<tr><th colspan="2">Principles</th></tr>
<tr><th>Federal Law on the Protection of Personal Data held by individuals (LFPDPPP)</th><th>APEC Privacy Framework</th></tr>
<tr><td>Legality.
<u>According to the article 7:</u>
Personal data must be collected and processed in a lawful manner in accordance with the provisions established by this Law and other applicable regulations.

Personal data must not be obtained through deceptive or fraudulent means.

In all processing of personal data, it is presumed that there is a reasonable expectation of privacy, understood as the trust any one person places in another for personal data provided to be treated pursuant to any agreement of the parties in the terms established by this Law.</td><td></td></tr>
</table>
</td></tr>
</table>

Economy	Does your economy consider or is your economy developing domestic privacy frameworks that refer to the APEC Privacy Framework (in particular, during the TFAP II period, 2007-2010)?	Provide how the APEC Privacy Framework (e.g., domestic legislation or guidelines, etc.) is referred to or any other information that can show the impact of the policy work of the DPS on the development/improvement of the data privacy system in your economy.	
		Consent: According to the article 8: All processing of personal data will be subject to the consent of the data owner except as otherwise provided by this Law. Consent will be express when such is communicated verbally, in writing, by electronic or optical means or via any other technology, or by unmistakable indications. It will be understood that the data owner tacitly consents to the processing of his data when, once the privacy notice has been made available to him, he does not express objection. Financial or asset data will require the express consent of the data owner, except as provided in Articles 10 and 37 of this Law. Consent may be revoked at any time without retroactive effects being attributed thereto. For revocation of consent, the data controller must, in the privacy notice, establish the mechanisms and procedures for such action.	Choice
		Information According to the article 9: In the case of sensitive personal data, the data controller must obtain express written consent from the data owner for	Notice

Economy	Does your economy consider or is your economy developing domestic privacy frameworks that refer to the APEC Privacy Framework (in particular, during the TFAP II period, 2007-2010)?	Provide how the APEC Privacy Framework (e.g., domestic legislation or guidelines, etc.) is referred to or any other information that can show the impact of the policy work of the DPS on the development/improvement of the data privacy system in your economy.	
		processing, through said data owner's signature, electronic signature, or any authentication mechanism established for such a purpose. Databases containing sensitive personal data may not be created without justification of their creation for purposes that are legitimate, concrete and consistent with the explicit objectives or activities pursued by the regulated party.	
		Quality According to the article 11: The data controller shall ensure that personal data contained in databases is relevant, correct and up-to-date for the purposes for which it has been collected. When the personal data is no longer necessary for the fulfillment of the objectives set forth in the privacy notice and applicable law, it must be cancelled. The controller of the database will be required to remove information relating to nonperformance of contractual obligations, after a period of seventy-two months counted from the calendar day on which said nonperformance arose.	Integrity
		Purpose According to the article 13:	Collection Limitation

Economy	Does your economy consider or is your economy developing domestic privacy frameworks that refer to the APEC Privacy Framework (in particular, during the TFAP II period, 2007-2010)?	Provide how the APEC Privacy Framework (e.g., domestic legislation or guidelines, etc.) is referred to or any other information that can show the impact of the policy work of the DPS on the development/improvement of the data privacy system in your economy.	
		Processing of personal data will be done as necessary, appropriate and relevant with relation to the purposes set out in the privacy notice. In particular, for sensitive personal data, the data controller must make reasonable efforts to limit the processing period thereof to the minimum required**.**	
		Loyalty According to the article 14: The data controller shall ensure compliance with the personal data protection principles established by this Law, and shall adopt all necessary measures for their application. The foregoing will apply even when this data has been processed by a third party at the request of the data controller. The data controller must take all necessary and sufficient action to ensure that the privacy notice given to the data owner is respected at all times by it or by any other parties with which it has any legal relationship.	Preventing Harm
		Proportionality According to the article 13:	Uses of personal information

Economy	Does your economy consider or is your economy developing domestic privacy frameworks that refer to the APEC Privacy Framework (in particular, during the TFAP II period, 2007-2010)?	Provide how the APEC Privacy Framework (e.g., domestic legislation or guidelines, etc.) is referred to or any other information that can show the impact of the policy work of the DPS on the development/improvement of the data privacy system in your economy.
		Processing of personal data will be done as necessary, appropriate and relevant with relation to the purposes set out in the privacy notice. In particular, for sensitive personal data, the data controller must make reasonable efforts to limit the processing period thereof to the minimum required.
		Accountability According to the article 19: All responsible parties that process personal data must establish and maintain physical and technical administrative security measures designed to protect personal data from damage, loss, alteration, destruction or unauthorized use, access or processing. Data controllers will not adopt security measures inferior to those they keep to manage their own information. Moreover, risk involved, potential consequences for the data owners, sensitivity of the data, and technological development will be taken into account.
New Zealand	Yes	The New Zealand Law Commission is scheduled to release recommendations in July 2011 to reform the Privacy Act 1993. It is expected that they will propose to amend the law to allow for the future adoption of cross-border privacy rules system (i.e. the proposed APEC system) in New Zealand. [Update: Please see

Economy	Does your economy consider or is your economy developing domestic privacy frameworks that refer to the APEC Privacy Framework (in particular, during the TFAP II period, 2007-2010)?	Provide how the APEC Privacy Framework (e.g., domestic legislation or guidelines, etc.) is referred to or any other information that can show the impact of the policy work of the DPS on the development/improvement of the data privacy system in your economy.
		http://privacy.org.nz/new-zealand-law-commission-privacy-review/.]
Peru	Yes.	The protection of data privacy is a constitutional right, which is recognized under Article 2, Item 6 of Peruvian Political Constitution, which states that "Every person has the right that the information services do not provide information affecting personal and familiar intimacy". In addition, the right to inviolability of communications and private documents is established under Article 2, Item 10 of Peruvian Political Constitution. Besides its constitutional protection, Peru has recently developed a legal framework for the protection of data privacy. Currently, Peruvian Congress has approved the Law on Personal Privacy Protection and its enactment is expected shortly. The main elements of the Law mentioned above are referred to the following aspects: (i) the legal qualification of "Personal Data" and "Sensitive Data", (ii) the principle of previous consent for the treatment of personal data by data banks, (iii) the creation of a national authority competent for the protection of personal data, and (iv) the regulation of personal data banks. In developing domestic data privacy rules, Peru has used as an important input the information shared as part of the workshops and seminars related to the establishment of policy frameworks for the implementation of data privacy systems. Taking into account that the Law on Personal Data Protection will be enacted shortly, technical assistance provided in the context of DPS work, will be particularly relevant for the implementation of a data privacy system tailored to our economy.
Philippines	Yes	The Philippines is also developing its domestic data privacy framework that is aligned with the APEC Privacy Framework. Our data privacy bill has passed Third Reading in the House of Representatives and has started deliberation in the Senate. In the meantime that we still do not have a Data Privacy Law in the Philippines, the Department of Trade and Industry (DTI) issued Department Administrative Order No. 8 in 2006 "Prescribing the Guidelines for the Protection of Personal Information in ICT Systems in the Private Sector". Please note that the bills pending in Congress cover both the private and government sectors.

Economy	**Does your economy consider or is your economy developing domestic privacy frameworks that refer to the APEC Privacy Framework (in particular, during the TFAP II period, 2007-2010)?**	**Provide how the APEC Privacy Framework (e.g., domestic legislation or guidelines, etc.) is referred to or any other information that can show the impact of the policy work of the DPS on the development/improvement of the data privacy system in your economy.**
Singapore	Yes	Singapore is currently developing a data protection legislation, which is intended to be introduced for Parliament's consideration in 2012. As part of our research, we have studied data protection regimes as well as best international practices of key jurisdictions, organisations and groups. The APEC Privacy Framework has been considered as part of this research. Singapore has followed closely developments of the ECSG, in particular the CPEA, which will provide useful guidance on treatment and collaboration on cross-border enforcement
United States	Yes	The United States Department of Commerce recently issued a report detailing initial policy recommendations aimed at "promoting consumer privacy online while ensuring the Internet remains a platform that spurs innovation, job creation, and economic growth." This report calls for the adoption of a comprehensive baseline set of data privacy standards, based on the Fair Information Practice Principles (FIPPS), which were themselves the basis for the OECD Guidelines and the APEC Privacy Framework. In addition, this report emphasizes the importance of global privacy policy interoperability based on accountability. The APEC cross-border privacy rules system is specifically referenced as advancing this concept because it incorporates specified accountability requirements for participating businesses and provides for effective protection for consumers. The report specifically recommends that the United States should continue to support the APEC Data Privacy Pathfinder project as a model for the kinds of principles that could be adopted by groups of countries with common values but sometimes diverging privacy legal frameworks. Available at http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf