The Cross Border Privacy Rules System: Promoting consumer privacy and economic growth across the APEC region

05 September 2013

> APEC should be congratulated for being an early adopter of the concept. The APEC Privacy Framework is a key milestone in ensuring data privacy.

In today's digital economy, data is stored remotely and accessed anywhere in the world. Emails could be stored on servers in Australia by an American company and accessed in Singapore. Buyers and sellers across different time zones purchase goods, share personal data, and make financial payments via the internet.

These cross-border online data flows are an integral part of today's international trade and governments are working on how to regulate this data flow to both promote e-commerce and protect consumers' data privacy.

"The global online marketplace knows no boundaries. In a split second, data can move across borders with no regard to jurisdiction," said Daniele Chatelois, Chair of APEC's Data Privacy Subgroup under the Electronic Commerce Steering Group, which has spearheaded APEC's decade-long work in this area.

"Advancements in information and communications technologies have resulted in exponential increases in the speed and volume at which information can travel," explained Ms Chatelois.

This means personal data can be shared quickly across multiple users, increasing the chances of fraud and other risks. On the other hand, these technological advances also provide new business opportunities. There is a fine balance between protecting consumers' personal information and creating unnecessary barriers to the flow of information.

"APEC's Data Privacy Subgroup has been working to create a policy environment that favours free flow of information across borders while at the same time providing effective and meaningful protection for personal information, essential to trust and confidence in the online marketplace," said Ms Chatelois.

APEC's work began in 2005 when it established the APEC Privacy Framework, a trailblazer for its time. The Framework laid out a set of nine principles to assist APEC economies in developing data privacy approaches that optimize privacy protection and cross-border data flows. The Framework also provided technical assistance to APEC member economies that had not addressed data privacy from a regulatory or policy perspective and helped bridge the differences between those economies with data privacy rules in place.

"APEC should be congratulated for being an early adopter of the concept. The APEC Privacy Framework is a key milestone in ensuring data privacy," said Joseph Alhadeff, Vice President of Global Public Policy at Oracle, a leading software company, and Chair of the International

Latest Articles

14 Quotes from President Gabriel Boric of Chile at the APEC CEO Summit
San Francisco, The United States | 13 December 2023

13 Quotes from President Ferdinand E. Marcos, Jr of the Republic of the Philippines at the APEC CEO Summit
San Francisco, The United States | 13 December 2023

In order to implement the APEC Privacy Framework, APEC developed the Cross-Border Privacy Rules (CBPR) system. The APEC CBPR system is designed to protect the privacy of consumer data moving between APEC economies by requiring companies to develop their own internal business rules on cross-border data privacy procedures.

Since 2008, APEC has been working on implementing its Cross Border Privacy Rules system.

“In 2008, a work plan detailing nine projects necessary to implement the APEC Cross Border Privacy Rules (CBPR) system was introduced,” said Josh Harris, Chair of the APEC Cross-Border Joint Oversight Panel, charged with operationalizing the CBPR system.

“By 2011, all projects had been completed and the Cross-Border Privacy Rules (CBPR) system became a reality,” added Mr Harris. “In 2012, the United States and Mexico became the first economies to join the system and put it into practice.”

Further, APEC Leaders, in their 2011 Declaration, committed to the implementation of the CBPR system as part of a number of steps to further open markets and facilitate regional trade.

The APEC Cross-Border Privacy Rules (CBPR) system makes use of “accountability agents” or third parties that verify an organization’s data privacy policies and practices meet the APEC CBPR program requirements. In addition, regulators in participating economies are also required to have the ability to take enforcement action under domestic laws and regulations that have the effect of protecting personal data consistent with the CBPR system. This international group of regulators may work together to assist in data privacy-related investigations or enforcement matters through their participation in the APEC Cross-Border Privacy Enforcement Arrangement (CPEA).

“The privacy enforcement authorities in participating economies are an integral part of the CBPR system” said Blair Stewart, an assistant Privacy Commissioner from New Zealand and one of the APEC Cross Border Privacy Enforcement Arrangement (CPEA) Administrators. “They perform a ‘backstop regulator’s’ role in cases that require escalation from the accountability agents.”

“There are notable challenges to privacy enforcement in the cross-border e-commerce realm,” explained Mr Stewart. “But APEC is on the leading edge of tackling those challenges
gh the use of accountability agents in the CBPR system and the creation of the
ateral Cross-Border Privacy Enforcement Arrangement (CPEA) through which
rities can request assistance in any privacy case – and not just CBPR cases.”

To date, 23 regulators from 8 economies have joined this regional enforcement arrangement.

Since the United States became part of the APEC’s Cross Border Privacy Rules system (CBPR) in 2011, TRUSTe was named as an authorized accountability agent and the Federal Trade Commission has been designated as the main enforcement authority.

In August 2013, IBM was the first US company to be certified under the APEC Cross-Border Privacy Rules (CBPR) system. TRUSTe, the accountability agent, approved IBM’s compliance with APEC data protection standards.

For IBM, joining the CBPR system is a way to demonstrate to potential clients and consumers that they are a trustworthy and accountable company for handling personal information. As more organizations and economies participate in the CBPR system, consumers will benefit from consistent data privacy protections across the APEC region regardless of where their personal data is processed, moved or stored.

More economies are starting to join the APEC Cross-Border Privacy Rules (CBPR) system. In June 2013, Japan applied to participate in the CBPR system.

“As a critical step to bringing more member economies on board, the APEC multi-year capacity building project helps economies come up to speed with the Cross-Border Privacy Rules system,” said Mr Harris, who is also the APEC Project Overseer.

“For example, the APEC capacity building project helps economies select an accountability agent to certify companies or provides other assistance to facilitate a member’s readiness to adopt the Cross-Border Privacy Rules system,” adds Mr Harris.

Still, there are many challenges to ensuring the free flow of data across borders while making sure this information remains protected. The next step is to use the CBPR system as a means to facilitate cooperation among diverse national and regional privacy and data protection regimes. The APEC Data Privacy Subgroup is currently working with the European Union to explore inter-regional cooperation. The Joint APEC-EU Working Team has begun to map the respective systems, identify differences, and help develop practices that could apply to both systems.

“When you think about privacy, it’s a construct based on cultural norms and has a personal dimension. The Internet and the cloud are global in scope and deployment but have local personal and legal implications,” explained Mr. Alhadeff.