Enabling Legal Compliance & Cross-Border Data Transfers with the APEC Cross-Border Privacy Rules (CBPR)

18 July 2016
Singapore

Electronic Commerce Steering Group

Produced By

Markus Heyder mheyder@hunton.com
Centre for Information Policy Leadership at Hunton & Williams LLP
2200 Pennsylvania Avenue, NW
Washington, DC 20037
Tel: 202-955-1563
Email: information@hunton.com
Website: www.hunton.com or www.informationpolicycentre.com

For
Asia-Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace
Singapore 119616
Tel: (65) 68919 600
Fax: (65) 68919 690
Email: info@apec.org
Website: www.apec.org

APEC#216-CT-04.2

Table of Contents

An APEC & CIPL workshop for information controllers, information processors and regulators in the Asia-Pacific region.

Enabling Legal Compliance & Cross-Border Data Transfers with the APEC Cross-Border Privacy Rules (CBPR)

Monday, 18 July 2016
Singapore

Workshop Report

I. Introduction

Information privacy and the free flow of data in the Asia-Pacific region have been one of APEC's priorities for more than a decade now. In 2005, APEC, through the Electronic Commerce Steering Group (ECSG) and its Data Privacy Subgroup (DPS), completed the APEC Privacy Framework (Framework) that set forth nine high-level privacy principles and guidance on domestic and international implementation. The Framework included a mandate for the APEC Member Economies to develop a cross-border privacy rules system for businesses to "facilitate responsible and accountable cross-border data transfers and effective privacy protections without creating unnecessary barriers to cross-border information flows, including unnecessary administrative and bureaucratic burdens for businesses and consumers."[1]

After a multi-year, multi-stakeholder negotiation process, the 21 APEC Member Economies endorsed the "APEC Cross-Border Privacy Rules" or "CBPR" system and began the currently ongoing implementation process across the Member Economies. To participate in the CBPR system, individual Member Economies must meet certain requirements, such as having at least one Privacy Enforcement Authority (PEA) that is able to enforce the CBPR against participating businesses and at least one Accountability Agent (AA) that will review and certify companies under the CBPR before they can participate. If they meet the basic pre-requisites for participation, Member Economies that wish to participate must formally join the CBPR system. Once an economy has joined the CBPR and has designated at least one AA, businesses in that economy may seek CBPR certification from the AA. Once a business is CBPR certified, it must comply with the specific privacy and information security program requirements of the CBPR.

To date, four APEC Economies have joined the CBPR system – the United States, Mexico, Japan and Canada. Other economies are currently considering and taking steps to join the system in the future. Only the United States and Japan so far have designated their AAs – TRUSTe for the US, and JIPDEC for Japan. Both AAs are accepting applications for CBPR participation by businesses. So far, there are about 16 CBPR certified companies and many more in the application pipeline.

In 2015, the APEC Economies also endorsed the APEC Privacy Recognition for Processors (PRP), which is a cross-border privacy code of conduct specifically for information processors

[1] APEC Privacy Framework, part iv. Implementation, Part B.III.48

that the APEC Economies developed following the completion of the CBPR. To date, no APEC Economy has joined the PRP.

In order to increase awareness and knowledge about the purposes and functioning of the CBPR system among government and private sector stakeholders and to help develop Member Economies' domestic capabilities to implement the CBPR system, APEC has established a multi-year funding project for CBPR capacity-building initiatives (MYP). The 18 July 2016, CBPR workshop in Singapore that is the subject of this Report was organized by the Centre for Information Policy Leadership (CIPL) under the auspices and in furtherance of the MYP. Given that the CBPR and PRP are related and complementary systems, they were both covered at the workshop.

Approximately 100 participants attended the workshop.

II. Welcome and Scene Setting

Piet Grillet, General Counsel of MasterCard Asia Pacific, opened the workshop. The conferencing facilities were graciously provided by MasterCard. Mr. Grillet noted that cross-border data transfers must have the appropriate level of protection and welcomed the development of the CBPR system towards that end.

Bojana Bellamy, President of CIPL, added in her welcoming remarks that developing the CBPR and similar accountability systems is particularly important for building bridges in a world of fragmented privacy regimes as well as for creating reliable transfer mechanisms and cross-border privacy protections in APEC and globally.

Zee Kin Yeong, Assistant Chief Executive of the Personal Data Protection Commission Singapore (PDPC), discussed the broader context of the CBPR from a Singaporean perspective, noting Singapore's desire to become the first "smart nation" based on innovative and effective use of information. He emphasized that this goal can only be accomplished when information can flow freely and accountably across borders. He noted the importance of building public trust through responsible information management and use practices.

III: Session I: CBPR Basics – What They Are and How They Work

Markus Heyder, Vice President and Senior Policy Counselor of CIPL and **Joshua Harris**, Director of Policy at TRUSTe, provided a basic introduction into the CBPR and the PRP to ensure that all participants have a common baseline of understanding for the more in-depth sessions on specific CBPR topics in the afternoon.

Zee Kin Yeong, of the PDPC discussed the PDPC's current deliberations about how Singapore could implement and participate in the CBPR. He commented on the specific potential benefits of the CBPR for Singapore and local businesses as well as addressed some of the legal and other issues that remain to be resolved in terms of Singapore's participation in the system, such as how enforcement and oversight would work.

IV. Session II: From an All-APEC Transfer System to a Global Transfer System

Jacobo Esquenazi, Global Privacy Strategist at HP, Inc., moderated a panel designed to cover a range of issues relating to the implementation and growth of the CBPR and PRP systems within the APEC region and connecting the APEC systems to non-APEC cross-border transfer systems, such as the European Union's Binding Corporate Rules (BCR). The comments of the panelists and audience signaled widespread interest in growing the CBPR and PRP systems more quickly as well as underlined the importance of making them interoperable with other systems to enable organizations' need for a global solution to global data flows.

Andrew Flavin, Policy Advisor, Office of Digital Service Industries, International Trade Administration at the US Department of Commerce, discussed the current state of implementation of the CBPR and PRP within APEC and highlighted some of the recent positive developments that indicate mounting interest among APEC economies to join the CBPR system. He also encouraged APEC economies to make use of the PRP, particularly those economies that have expressed a strong interest in an information processor rules system for APEC due to their significant domestic processing industries. Finally, he discussed the ongoing work between APEC and the EU to streamline dual applications and towards "interoperability" between the CBPR and BCR, such as by creating a common application form, a joint map of materials needed for demonstrating compliance, and a document mapping the BCR for processors to the PRP.

Bui Thi Thanh Hang, Vice Head, International Affairs Division, Viet nam E-commerce and IT Agency (VECITA) of the Ministry of Industry and Trade, described the ongoing CBPR implementation process in Viet nam as well as the outstanding issues that remain to be resolved in Viet nam, including the issue of government oversight and enforcement. Viet nam will hold a CBPR capacity building workshop in October 2016. She noted the substantial benefits Viet nam sees in the CBPR system.

Tsuzuri Sakamaki, Counselor, Personal Information Protection Commission (PPC) Japan, gave an overview over Japan's recent amendments to its privacy law, particularly as they relate to Japan's participation in the CBPR system. Japan will specifically provide for the CBPR to be one of the recognized mechanisms for data transfers under its new regime of data transfer restrictions, whereby data may be transferred to CBPR-certified organizations outside of Japan because they will have demonstrated company-level competency to receive Japanese personal information.

Hilary Wandall, AVP, Compliance and CPO for Merck & Co., Inc. discussed the value of accountability-based information management and cross-border transfer systems, such as the CBPR. She also described how her organization's CBPR certification helped streamline its subsequent BCR approval in the EU, thereby validating the importance of the "interoperability" work currently in progress between the EU and APEC.

V. Session III: A Deep-Dive Into the Benefits of the CBPR – Why Companies Should Join

Markus Heyder, CIPL, moderated a panel designed to provide a close look at the specific advantages and benefits to companies that the CBPR and PRP systems will deliver. The issues touched upon by the panelists included considerations that are relevant for large multinational companies and SMEs. They also commented on how CBPR benefits may differ from jurisdiction to jurisdiction and how a CBPR certification can be leveraged to streamline approval of an organization's BCR in the EU.

Annelies Moens, Deputy Managing Director at Information Integrity Solutions, provided the participants with an overview over her recent study of CBPR benefits entitled "Preliminary assessment: Potential benefits for APEC economies and businesses joining the CBPR system," which provided a detailed analysis of the numerous benefits of the CBPR from the vantage point of the various stakeholders, ranging from governments, businesses and regulators. She emphasized the importance of further awareness-raising related to the CBPR system, as there still appears to be widespread lack of knowledge among stakeholders that might benefit from the CBPR. She also touched on the issue of providing incentives to businesses to seek CBPR certification, especially in jurisdictions that do not yet have data transfer restrictions and where the immediate need for CBPR might, therefore, not be apparent.

Daisuke Nagasaki, Deputy Director, International Affairs Office, Commerce and Information Policy Bureau in the Ministry of Economy, Trade and Industry, Japan (METI), described Japan's rationale for joining the CBPR system, noting that the CBPR will be placed under Japan's recently amended Personal Information Protection Act, which will be fully implemented by September 2017, as a tool to prove adequacy at a company level for purposes of cross-border personal data transfers. For that reason, he urged other APEC economies to join the system as well. He also emphasized the function of the CBPR to demonstrate corporate social responsibility on the part of a company.

Jacobo Esquenazi, HP, Inc., explained why HP Inc. obtained CBPR certification. Among other reasons, such as the increase in APEC economies that prohibit transfers absent participation in some mechanism such as the CBPR, he noted how they aligned with and enabled HP's information management and use culture that is based more on an accountability model than a liability model. He noted that data must move for business reasons rather than legal reasons. Participating in the CBPR system enables that approach while also enabling stronger privacy protections, particularly when more APEC economies join the CBPR and PRP systems, more companies become certified, and the APEC transfer systems connect to other non-APEC transfers systems.

Harvey Jang, Director, Global Privacy & Data Protection at Cisco described the rationales of Cisco for seeking CBPR certification. The benefits in joining the system included (1) demonstrating legal compliance and accountability; (2) external validation and testing by a third party; (3) global interoperability and consistency; (4) meeting employee and customer expectations; and (5) building and enhancing trust. He also noted competitive differentiation as one of the benefits of CBPR participation.

Huey Tan, Senior Privacy Counsel at Apple stressed the importance and tremendous potential of a trust-based data transfer network for APEC and beyond. Noting the cultural affinity between some of the Asian economies and the CBPR's "communal" approach to data protection, he urged APEC economies to more quickly embrace and build-out this system so that it can become a viable mechanism for businesses of all sizes in the region and a stepping stone for a global approach to accountable data transfers.

VI. Session IV: A Deep-Dive into the Certification Process

Markus Heyder, CIPL, moderated a panel of Accountability Agents and Privacy Officers on what to expect during the CBPR certification process. The purpose of this panel was to advise interested companies on the particular steps involved in obtaining certification and maintaining it. It was also important to show how the pre-existing level of compliance and privacy preparedness of an organization impacts the CBPR certification process in terms of difficulty and length as well as how the AA can help companies that do not yet have fully formed internal privacy programs in place to develop such programs.

Josh Harris, TRUSTe, described TRUSTe's CBPR certification process, explaining in detail the necessary steps starting with the initial application and the types of questions and issues the applicants must address and how they must address them, to the ongoing monitoring requirements and the annual recertification process. He also described how TRUSTe works with the individual applicants to get their internal privacy programs into compliance with the CBPR program requirements.

Hiromu Yamada, CBPR Certification Business Office, Japan Institute for Promotion of Digital Economy and Community (JIPDEC), explained JIPDEC's planned CBPR certification process, as JIPDEC has not yet begun to review organizations for participation. JIPDEC has a long history of providing certifications and is in the process of adapting its existing processes for the CBPR context. JIPDEC is ready to receive applications for CBPR certification.

As representatives of two CBPR-certified companies, **Jacobo Esquenazi**, HP, Inc., and **Hilary Wandall**, Merck, discussed their personal experiences with the CBPR certification process. They both stressed how the relative burdensomeness of this process depends on how advanced an organization is in terms of having a comprehensive accountability-based information management and privacy infrastructure in place already. Given the significant overlap of requirements between the CBPR and BCR, they also discussed how being certified or approved under one of these systems can be leveraged for a simpler approval process in the other system.

Jacobo Esquenazi, HP, Inc., explained why HP Inc. obtained CBPR certification. Among other reasons, such as the increase in APEC economies that prohibit transfers absent participation in some mechanism such as the CBPR, he noted how they aligned with and enabled HP's information management and use culture that is based more on an accountability model than a liability model. He noted that data must move for business reasons rather than legal reasons. Participating in the CBPR system enables that approach while also enabling stronger privacy protections, particularly when more APEC economies join the CBPR and PRP systems, more

companies become certified, and the APEC transfer systems connect to other non-APEC transfers systems.

Harvey Jang, Director, Global Privacy & Data Protection at Cisco described the rationales of Cisco for seeking CBPR certification. Harvey noted that the CBPR requirements are consistent with most other privacy frameworks – OECD, FIPs, BCR, GDPR, Privacy Shield, etc. Obtaining CBPR certification was part of validating and getting external recognition for Cisco's privacy and data protection program (Cisco was certified this month).The benefits in joining the system included (1) demonstrating legal compliance and accountability; (2) efficient and cost-effective external assessment and testing by an independent third party; (3) global interoperability and consistency; (4) meeting employee and customer expectations; and (5) building and enhancing trust. He also noted competitive differentiation as one of the benefits of CBPR participation.

Huey Tan, Senior Privacy Counsel at Apple stressed the importance and tremendous potential of a trust-based data transfer network for APEC and beyond. Noting the cultural affinity between some of the Asian economies and the CBPR's "communal" approach to data protection, he urged APEC economies to more quickly embrace and build-out this system so that it can become a viable mechanism for businesses of all sizes in the region and a stepping stone for a global approach to accountable data transfers.

VII. Session V: Enforcing the CBPR

Bojana Bellamy, CIPL, moderated a session on the enforcement structure behind the CBPR system, including the system that APEC privacy enforcement authorities have created to cooperate with each other across the different APEC jurisdictions. The purpose of this panel was also to highlight the importance of robust enforcement, including addressing false CBPR claims in an appropriate and consistent way through effective governance of the CBPR system to maintain its credibility to the public and value to the participating businesses and other stakeholders.

Melinda Claybaugh, Counsel for International Consumer Protection, Office of International Affairs, US Federal Trade Commission, stressed the importance of strong enforcement to the ultimate success of the CBPR system. She underscored that maintaining the credibility of the CBPR system will be crucial to developing and preserving the public trust in the system, as well as the value of investment of companies that have certified to the CBPR. She also discussed the FTC's first CBPR-related enforcement initiatives against businesses that had falsely claimed in their privacy policies that they are CBPR-certified. In addition, she noted that the issue of how to combat false claims relating to CBPR certification throughout the CBPR system may have to be further discussed within the APEC DPS to ensure that all participating member economies not only have the capability to enforce the CBPR's substantive program requirements but also to combat false claims associated with the CBPR.

Andrew Flavin, US Department of Commerce, described possible ways forward through the DPS, a DPS working group and/or the CBPR Joint Oversight Panel (JOP) with respect to a number of enforcement, complaint-handling and dispute resolution-related issues that could be further improved and streamlined. For example, he discussed how it is in all stakeholders'

interest to ensure that consumers have an effective and centralized mechanism to log complaints and suggested that the current mechanism found on the CBPR website, www.cbprs.org, might be further refined and improved. Both panelists emphasized the utmost importance of addressing these issues at the early stages of CBPR implementation to avoid bigger problems at a later stage.

VIII. Conclusion

By all accounts, the CBPR workshop appeared a success in terms of wide participation by businesses, governments, regulators and other stakeholders, the wide range of issues covered, and the active engagement by the participants during the panel discussions. A sentiment expressed frequently throughout the day was the need to implement the CBPR system across APEC as quickly as possible to enable its full range of benefits for businesses, governments, privacy authorities and consumers.

Participants also identified a number of key issues that need to be clarified by APEC in the near term, such as, for example, (1) the rules around selecting the relevant jurisdiction for certification for companies (and their subsidiaries) that are active in numerous APEC Member Economies and/or that are headquartered outside of APEC but with significant business operations in APEC, and the precise scope of a CBPR certification in these cases; and (2) how false claims relating to CBPR certification can be enforced against in the various APEC Member Economies.

Finally and importantly, a key message from the workshop was the urgent need for additional public education on the purposes, benefits and workings of the CBPR system. Many stakeholders, including APEC-based governments, regulators, privacy authorities and businesses, are still unsure about key elements of the CBPR/PRP systems and continue to request more user-friendly, easy-to-understand information about these systems to enable their deliberations about whether and how to participate in the CBPR/PRP systems.

Asia-Pacific
Economic Cooperation