Bloomberg BNA

Privacy and Security Law Report®



Data Protection

# APEC Privacy Rules for Cross-Border Data Flows—A Model for Global Privacy Protections

By Anick Fortin-Cousens and Markus Heyder

*Anick Fortin-Cousens is program director in IBM's Corporate Privacy Office, where she leads a team responsible for IBM's global privacy policies and programs and serves as IBM's Privacy Officer for Canada, Latin America, the Middle East & Africa. She also chairs Hunton & Williams LLP's Centre for Information Policy Leadership's Asia Subgroup and is actively involved in the work of the Information Accountability Foundation.*

*Markus Heyder is vice president & senior policy counselor of Hunton & Williams' Centre for Information Policy Leadership. Previously, he was the Federal Trade Commission's principal staff representative in organizations and networks, including the APEC Data Privacy Subgroup, the Asia Pacific Privacy Authorities, the International Conference of Data Protection and Privacy Commissioners, the International Working Group on Data Protection in Telecommunications and the Global Privacy Enforcement Network..*

The Asia Pacific region has become a privacy hotbed in recent years, due in large part to privacy-related initiatives of the Asia Pacific Economic Cooperation (APEC)[1] forum. One of these initiatives was the development of the APEC Cross-Border Privacy Rules (CBPR)[2] for personal information controllers. With the creation of the CBPR, APEC not only created a privacy-protective mechanism for cross-border data transfers within its own region, but also a blueprint for a more far-reaching global scheme. While the CBPR system had a slow start following its 2012 launch, two developments should soon give it a boost: the recently-endorsed[3] complementary system for processors—the APEC Privacy Recognition for Processors (PRP)[4]—and the ongoing work on connecting the CBPR to the European Union's Binding Corporate Rules (BCR). Indeed, over the coming months, we may very well see more APEC economies initiating the process of joining the system and more companies seeking their CBPR (and soon PRP) certification.

[1] APEC, whose mission is focused on free trade and economic investment, comprises the following 21 member economies: the U.S., Canada, Mexico, Peru, Chile, New Zealand, Australia, China, Hong Kong, Russia, South Korea, Japan, Singapore, Vietnam, Malaysia, Philippines, Thailand, Papua New Guinea, Indonesia, Chinese Taipei and Brunei Darussalam. More information on APEC can be found on the organization's website, *available at* http://www.apec.org/.

[2] More information on the Cross-Border Privacy Rules system can be found athttp://www.cbprs.org/ (11 PVLR 55, 1/9/12).

[3] The Privacy Recognition for Processors was finalized and endorsed by APEC at its most recent Senior Officials Meeting in the Philippines in February 2015. The processor documents are available at http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx.

[4] Before processors can join, the PRP still has to be operationalized and integrated into the overall CBPR governance structure over the coming months.

 ISSN 1538-3423

## How the CBPR (and now PRP) System Works in a Nutshell

The CBPR system is straightforward.

In order to join, any APEC member economy must submit a formal declaration of its intent to participate in the system, demonstrate how the CBPR can be enforced under national law and identify at least one ''accountability agent,'' which is an APEC-recognized third party certifying organization.[5] Each participating economy must also have at least one domestic Privacy Enforcement Authority that is capable of enforcing the CBPR and that participates in the APEC Cross-border Privacy Enforcement Arrangement (CPEA).[6]

In order to participate in the system, accountability agents must meet rigorous recognition criteria that deal with conflicts of interest and outline their obligations on issues ranging from the initial assessment and certification process to ongoing monitoring of their certified companies and consumer complaint handling. Accountability agents must also be re-approved every year by the participating APEC member economies.

As for companies, they must apply to an accountability agent as a first step in order to participate in the CBPR. The accountability agent assesses the company's privacy policies and practices against the CBPR program requirements, requires adjustments and modifications where necessary and certifies the company. The program requirements track and implement the privacy principles set forth in the APEC Privacy Framework.[7] Once certified, the CBPR become enforceable against the company. Certified companies have to be re-certified annually.

Overlaying the entire CBPR system is a governance and operations structure led by a Joint Oversight Panel that is responsible for approving economy-level participation and managing accountability agent recognition.

It is expected that the PRP will follow the same model as the one aforementioned. [8]

## Status of CBPR Implementation and Next Steps

Three economies have joined the CBPR system since its inception—the U.S., Mexico and Japan—and Canada's accession should soon be confirmed. Others—such as South Korea, the Philippines, Thailand, Vietnam, Singapore, Hong Kong and Australia—have affirmed their interest and/or have taken steps towards participation. There is, however, only one APEC-recognized accountability agent thus far—TRUSTe—which means that only U.S.-headquartered companies can currently seek certification. Ten companies have been certified to date, and even more are under review by TRUSTe.

Still, while the CBPR system is up and running and its uptake accelerating, the system still needs to gain critical mass to fulfill its promise. More APEC economies need to participate, and more companies need to certify. The relevant APEC stakeholders are working on multiple tracks to facilitate the system's growth. With the recent endorsement of the processor system and the promising work toward interoperability with other regions, the prospects for growth are promising.

## The Case for CBPR and PRP

The original policy motivations for the CBPR system were threefold: (1) to provide a privacy-protective mechanism to transfer personal information across a region where national privacy laws might otherwise prohibit such transfers; (2) to introduce a degree of harmonization in a region of otherwise uneven and diverse privacy protections; and (3) to raise the general level of privacy protections.

With the recent proliferation of diverse privacy laws and data export restrictions in the APEC region, these motives have proven prescient. Cross-border transfer mechanisms such as the CBPR are now integral to an increasing number of cross-border transfer regimes. Witness Australia, where such schemes may be one way to continue to transfer data to other jurisdictions despite the transfer restrictions in their law. Consider the provisions in Singapore[9] that currently consider binding corporate rules, or binding corporate codes of conduct, such as the CBPR, as mechanisms under which personal information can be transferred overseas. Note also the recent Hong Kong guidance[10] on cross-border data transfers and the December 2014 outline of the soon-to-be-introduced new Japanese draft privacy bill, both of which accommodate mechanisms like the CBPR as a valid method for cross-border data transfers. The list of examples will only grow.

Besides serving as a recognized cross-border transfer mechanism, the CBPR provide numerous other benefits to all of its stakeholders—businesses, government and consumers.

**For governments, the case for CBPR and PRP participation can be made at the political and enforcement levels.**

For example, they enable businesses to show they have achieved a certain level of compliance with applicable privacy laws in the various participating APEC member economies. They also enable businesses to proactively demonstrate organizational accountability and good faith efforts to stakeholders, which can be leveraged in the event of an investigation or enforcement

[5] At the time of its endorsement, all 21 APEC economies formally expressed their general intention to join the CBPR system.

[6] Information about the CPEA can be found at http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx (8 PVLR 1653, 11/16/09).

[7] The APEC Privacy framework is available at http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx (4 PVLR 1476, 12/5/05).

[8] Due to the differences in national laws among APEC economies, PRP enforceability options and requirements differ from the more stringent enforceability requirements of the CBPR and the process by which APEC economies will articulate PRP enforceability in their jurisdiction is still under construction.

[9] Personal Data Protection Regulations 2014, § 10, *available at* http://bit.ly/1wdBTMb

[10] Hong Kong guidance is available at http://www.pcpd.org.hk/english/resources_centre/publications/guidance/files/GN_crossborder_e.pdf.

  PVLR ISSN 1538-3423

action. Mexico is an example of incorporating the use of such self-regulatory ''trust seals'' and code-of-conduct schemes into its privacy law to ''complement'' the law. Importantly, participating in such schemes also increases consumer trust. And, for companies taking a long-term view, an effective CBPR and PRP system also helps establish self- or co-regulatory regimes as viable alternatives to rigid, one-size-fits-all statutory privacy regimes.

For governments, the case for CBPR and PRP participation can be made at the political and enforcement levels. At the political level, they advance the two equally important objectives of privacy protection and trade. At the enforcement level, they enable more effective cross-border enforcement cooperation among the backstop enforcement authorities, streamline the investigatory process and augment the reach of compliance oversight through the frontline responsibilities of accountability agents.

Consumers also benefit, as these systems deliver more user-friendly complaint handling and overall better, more consistent and more easily enforceable privacy protections.

## Connecting APEC CBPR to Other Regions

Most companies interested in code-of-conduct schemes such as the CBPR and PRP are companies with a global or multi-regional footprint, or companies that wish to increase trust and attract foreign business beyond their region. Therefore, to maximize the true value of such schemes, stakeholders must think globally and interconnect the different regional variants. In fact, APEC is currently doing this at two levels: (1) at the practical level, through a joint working group of APEC privacy officials, Article 29 Working Party representatives and industry participants to explore opportunities for leveraging the commonalities between the CBPR and the EU BCRs into more efficient and streamlined dual certification and approval processes; and (2) at the framework level where, in the context of an ongoing ten-year review of the APEC Privacy Framework, APEC is considering ways to promote interoperability with frameworks outside of the APEC system.

The work of the joint EU-APEC working group toward greater interoperability is hugely important. After initially mapping the substantive requirements of the BCR and CBPR in the so-called Referential document of March 2014[11], the group subsequently conducted a series of company case studies on real-life experiences with dual certification. The result is a list of recommendations for concrete next steps toward streamlining the respective certification processes. On the table are proposals such as the development of a common application document for companies wishing to apply for both CBPR and BCR certification/approval, an agreed list of required supporting documentation and proof-points and a process for conveying such documents and other relevant information between the APEC accountability agents and the EU authorities responsible for approving BCR. If progress can be made on any of these proposals, the return for efficiency, and thus for privacy in general, will be significant.

## Conclusion

Much progress has been made in the implementation and advancement of the CBPR system through the PRP scheme, but more remains to be done. More APEC member economies must join the system they themselves created. They must also offer incentives for organizations to join. Additional accountability agents also have to be recognized. And as importantly, many more companies must certify and use the system to prove its viability. This will in turn help drive the ongoing work toward interoperability with the EU BCR and, ultimately, with other national and regional codes of conduct around the world. Indeed, APEC CPBR has contributed to the growing acceptance of delivering privacy protection through organizational accountability and codes of conduct. Even erstwhile CBPR critics are coming around. For example, following some recent clarifications and amendments to the certification process, Chris Connolly, chairman of the Australian Privacy Foundation International Committee, commenting on behalf of consumer and privacy organizations, called them a ''big win'' for the CBPR system.[12] Combined, these developments and opinion shifts have made what was once an uphill battle a little less steep and thus amenable and attractive to wider participation.

---

[11] ''Joint work between experts from the Article 29 Working Party and from APEC Economies, on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents'' (2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf (13 PVLR 431, 3/10/14).

[12] ''APEC Renews TRUSTe's Certification Role In Cross Border Data Transfer Privacy Plan,'' 14 Bloomberg BNA Privacy & Sec. L. Rep 207 (Feb. 2, 2015) (14 PVLR 207, 2/2/15).