Submission to the CBPR consultation

Consultation closes COB Thursday 27 July 2017

Your details

Name/organisation *(if you are providing a submission on behalf of an organisation, please provide the name of a contact person)*	Australian Information Industry Association
Contact details *(one or all of the following: postal address, email address or phone number)*	Suzanne Roche General Manager, Policy and Advocacy 0408232862 mailto:s.roche@aiia.com.au

Publication of submissions

In meeting the Australian Government's commitment to enhancing the accessibility of published material, the Attorney-General's Department will only publish submissions to this website that have been submitted electronically.

Please complete this template and send it to cbprconsultation@ag.gov.au.

If you choose to provide a separate document, the following formats are preferred:

- Microsoft Word
- Rich Text Format (RTF)
- txt format.

Please limit individual file size to less than 5MB. The department may create PDF documents from the above formats.

The department will still consider hardcopy submissions received by mail, but these submissions will not be published on the website.

Confidentiality

Submissions received may be made public on the Attorney-General's Department website unless otherwise specified. Submitters should indicate whether any part of the content should not be disclosed to the public. Where confidentiality is requested, submitters are encouraged to provide a public version that can be made available.

Would you prefer this submission to remain confidential? NO

Your submission

Insert your text here and submit it as an electronic Word document to cbprconsultation@ag.gov.au.

AIIA Submission to the APEC CBPR consultation

July 2017

Ground Suite B
7-11 Barry Drive
Turner ACT 2612

GPO Box 573
Canberra ACT 2601

T 61 2 6281 9400
E info@aiia.com.au
W www.aiia.comau

About AIIA

The Australian Information Industry Association (AIIA) is Australia's peak representative body and advocacy group for those in the digital ecosystem. AIIA is a not-for-profit organisation that has, since 1978, pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment and drive Australia's social and economic prosperity.

AIIA's members range from start-ups and the incubators that house them, to small and medium-sized businesses including many 'scale-ups' and large Australian and global organisations. We represent global brands including Apple, Adobe, Deloitte, Gartner, Google, HP, IBM, Infosys, Intel, Lenovo, Microsoft and Oracle; international companies including Optus and Telstra; national companies including Ajilon, Data#3, SMS Management and Technology and Technology One.

More than 90% of our members are SMEs.

Introduction

AIIA urges the Government to take a leadership role by clearly indicating its intention to participate in the APEC CBPR system without delay, as it committed to do in the 2011 APEC Leaders' Declaration. [1]

AIIA strongly supports Australian CBPR participation because:

- CBPR offers a degree of *harmonisation* in a region of uneven and diverse privacy protections[2]
- CBPR is a relatively *streamlined and flexible framework* that will not impose overly onerous regulatory or cost burdens on companies
- CBPR is *enforceable and potentially interoperable* with other global privacy regimes, for example in the EU
- CBPR is *voluntary* for companies to join in a participating economy
- There are no legal impediments to Australia participating
- As CBPR participants increase, managing personal information transfers will become *more efficient*, saving compliance costs and boosting consumer confidence in the digital economy
- CBPR is *sector neutral* – it will benefit all data transfer companies such as finance, telcos, pharmaceutical and health companies.

All APEC countries have made a commitment at the highest level of government to develop cross-border privacy rules for the APEC region and to use them once they exist to enhance privacy protection and eliminate barriers to cross-border data flows to facilitate trade. It is incumbent on governments in APEC economies to devise effective domestic strategies to implement these commitments and incentivise businesses to use the system.

---

[1] This Declaration states; "We will take the following steps to further open markets and facilitate regional trade: …

- Implement the APEC Cross Border Privacy Rules System to reduce barriers to information flows, enhance consumer privacy, and promote interoperability across regional data privacy regimes."

[2] Differing privacy mechanisms across the region pose compliance challenges. Varied and incompatible approaches nations are adopting to regulate data transfers are evident;18 of the 21 Asia Pacific Economic Community (APEC) economies now have sectoral or general Privacy Laws, 17 of which impose conditions on cross-border data flows.

Participating in the CBPR

Participation in the CBPR will facilitate Australia's global competitiveness in a complex regional trading environment, and indicate compliance with the APEC goal of sustainable economic growth and prosperity in the Asia Pacific region. Already, with the recent participation of Korea, there are five APEC economies now in the CBPR. Taiwan has announced its intention to join and Singapore is expected soon. At least six more economies are signalling their intention to join or watching progress. Twenty-one companies (including SMEs) are certified in the US, one in Japan, and Accountability Agents are established in each of Japan and the US. Momentum will continue to build. Australia is being left behind and showing leadership by joining will significantly improve the chance of successful implementation of the scheme. Although the CBPR system is up and running and its uptake accelerating, the system needs to gain critical mass to fulfil its promise. Australia's participation as a major APEC economy is fundamental to this outcome.

The APEC regional sector is critical to Australian trade for SMEs as well as larger corporations: retail consumers in the Asia-Pacific alone purchase around USD 1 trillion worth of goods and services online annually, accounting for just over half of global spend and with growth surging. It is a trend that is opening up vast digital online trade opportunities and underscores the importance of the robust protection of data. Trade examples include identity numbers, bank account and credit card information, medical records, travel documents, email and instant message content.

Global data flows are the product of increasing globalisation and digitisation of business processes and societal demands for online transacting. They are foundational to the modern economy – the ability to use, share and access information across borders enables data-driven services, fuels economic growth and increasingly is a lifeline for remote communities in developing nations.

Under the APEC Cross-Border Privacy System, privacy policies and practices of companies operating in participating APEC economies follow a set of commonly agreed rules based on the **APEC Privacy Framework**. Such companies are assessed and certified by a third-party accreditor known as an Accountability Agent. By aligning the domestic privacy laws of participating APEC economies, the system reduces barriers to information flows that underpin digitally-based trade between them. Firms certified by a recognised Accountability Agent are free to promote their adherence to the system's privacy standards as a way of building trust with customers and business partners. The system is designed to promote confidence in the online marketplace by deterring threats to data privacy and security. In doing so, it facilitates data flows increasingly central to people's daily lives, shaping the future of regional economies.

The growth and development of everything from apps, cloud computing and social media to biometrics, GPS information and online payments ultimately depends on a secure operating environment that APEC is seeking to ensure. As e-commerce expands opportunities for businesses big and small, it is imperative that policies enable transfers of data necessary for them to capitalise on growth, and for APEC economies to build their own economic, regulatory and social capacities.

AGD Questions

1. ***Would it be advantageous to Australian business and consumers for Australia to join the CBPR system?***

Yes. With each economy having its own privacy regulation and most organisations using cross-border operations, the costs can be significant to ensure compliance with legislation each time business is started in a new jurisdiction and implementing appropriate processes and controls. The cost can discourage businesses and lead to non-compliance. Although the transferor must continue to comply with its local privacy and data protection legal requirements, CBPR participation will provide a low-friction way in which companies can meet those requirements. Participation will also be beneficial for companies seeking a competitive advantage by

increasing trust and confidence that their cross-border transfers will be safe. The CBPR-certified company remains accountable for the protection of the information at the level of the originating APEC country regardless of where the data is transferred. So this is an added consumer benefit.

Another advantage of CBPR is that it allows transfers not only within a global corporate group (with Binding Corporate Rules –BCR)), but also between unaffiliated companies and to companies that are not CBPR-certified anywhere in the world. Non-APEC countries that adopt similar mechanisms could make their cross-border rules mechanisms interoperable with the CBPR (and other similar schemes). This will have the effect of creating a global certification mechanism requiring only one approval process. Certification demonstrates a commitment to consumer privacy and provides credible evidence of trustworthiness which may also help to attract future business from individuals and organisations in other APEC economies and, indeed, anywhere in the world.

CBPR requires critical mass. As more countries join and the number of participants increase, and as the CBPR integrates with other global systems, managing transfers of personal information will become more efficient, improving privacy and information management governance. As mentioned, there are only two Accountability Agents in the US and Japan so far. To make APEC CBPR more robust and reliable, adding more Accountability Agents will be necessary and such additional Agents will contribute to establishing the CBPR community and facilitating good practice under CBPR. By participating in the CBPR system and adding new Accountability Agent(s) to the process, Australia can provide diversity to the CBPR scheme and contribute to the making of more reliable framework for trans-border data flow.

2. ***Has Australia's lack of participation in the CBPR system hindered your business relations in the APEC region, or beyond? Why?***

A more relevant query here would address commercial opportunities foregone due to regulatory uncertainty for those organisations considering regional trade activity with APEC economies. Foregone opportunity cannot be measured, but to the extent member companies engage in the APEC region, they have indicated that they consciously assume additional risk in the current regional regulatory diversity. Risk is commercial anathema and will hinder robust trade and business relations.

The current commercial practice of using contract law to protect data transfer to regional jurisdictions is of necessity more complex and costly for all parties than a harmonised regulatory framework.

3. ***What is your experience in dealing with businesses in other APEC economies that are a part of the CBPR system?***

To date, the US and Japan are the most active participants, as Canada, Mexico and South Korea are still preparing for the implementation of the CBPR system. The US has no general regulation on cross border data flow. Japan's privacy provision is similar to the EU (personal data can be exported to "white listed" countries or to a country with substantially equal protection). But notably Japan interprets the provision as allowing personal data transfers (even if an export is to a non-APEC country) so long as the transfer is made by a CBPR participant company.

4. ***Would you be prepared to contribute to the cost of establishing and maintaining an Accountability Agent system?***

Members support the concept of user pays and would agree to bearing the costs of their own use of any Accountability Agent established in Australia. Organisations seeking to operate as Accountability Agents should contribute to the cost of their establishment and enrolment in the System and the organisations that are certified by Accountability Agents should absorb the costs of doing so.

5. ***Would you be prepared to contribute to the cost of the development and maintenance of additional enforcement arrangements (such as those that might be established through a code)?***

AIIA would be prepared to participate in the preparation of a Code to govern Australia's participation in the CBPR system, so long as it is a relatively simple activity and not a significant impost on industry or government resources. Guidelines for code development exist and OAIC, the body charged with the administration of privacy regulation, is already part of the CPEA. The need for "additional enforcement arrangements" should therefore be minimal.

6. ***What accountability and redress mechanisms do you think are appropriate for consumers dealing with businesses operating under the CBPR system?***

Consumer redress is adequately covered in the CBPR. Any enforcement necessary will ordinarily be carried out by the Accountability Agent, with the Privacy Enforcement Authority (PEA, in Australia, the OAIC) acting as a backstop, in the following sequence:

- the Accountability Agent discovers that a CBPR-certified company is not complying with the CBPR program requirements either through its regular monitoring or a complaint
- the Accountability Agent notifies the company, outlining remedial steps required to be undertaken within a reasonable period of time
- the Accountability Agent can take a number of enforcement actions, depending on the harm or potential harm. It can:
    1. remove the company from the CBPRS;
    2. suspend the company's right to display the accountability agent seal;
    3. name the company and publicise its non-compliance; or
    4. impose monetary penalties, or order compensation to harmed individuals.

If the issue is not resolved by the Accountability Agent, and there is a breach of local privacy law, the matter may be referred to the Privacy Enforcement Authority for review and action. Importantly for consumers, each participant is certified as compliant with the APEC CBPR System requirements. This occurs when the participant joins the System and thereafter on an annual basis. Unlike other transfer mechanisms where parties typically rely on the recipient to comply fully with contractual provisions, the rigour of the certification process demonstrates to consumers that an independent third party has certified that appropriate processes and controls are actually in place.

Conclusion

There are no legal impediments to Australia's immediate commitment to participate in CBPR. As an APEC member, Australian participation in CBPR framework is urgently required. Global trade and economic growth cannot continue to trend upwards without a trusted framework for privacy. Trade benefits are decisive considerations in the uptake of CBPR and trade is increasingly dependent on data and transfer of personal information, especially as service industries continue to grow and value is derived from the analysis and application of data. Australian SMEs are especially active in service industry trade in the Asian region.

CBPR, once it meets critical mass, will contribute to supporting advancement towards global trade and APEC's economic growth policy objectives by providing a scalable baseline set of privacy standards. It also has the potential to become interoperable with other international data protection frameworks, such as the EU BCR framework.

Adopting regional baseline standards such as the CBPR System has the potential to make the transition smoother when entering new markets and complying with increased privacy obligations. Having a common set of baseline standards which are interpreted in the same way will help overcome regulatory uncertainty that would otherwise make cross-border data transfers even more complex.

Consumers are adequately protected under CBPR with the dual processes of the Accountability Agent and the domestic privacy regulator (OAIC) being available to manage any breaches, with certification being evidence of audited compliance by the company with the APEC CBPR requirements.