APEC's Cross-border privacy rules system: A house of cards?

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia

(2014) 128 *Privacy Laws & Business International Report*, 27-30

APECs Cross-border privacy rules system (CPBRs) has been under development at least since 2007, after the APEC Privacy Framework was completed in 2005.[1] The proponents of APEC CBPRs present it as having a major role in the Asia-Pacific, and in transfers of personal data globally, particularly between the EU and the Asia-Pacific. Different views are possible, but it needs to be examined and debated in considerable detail. I suggest scepticism, and that APEC CBPRs may turn out to be a house of cards.[2]

Contrasting views

The EU's Article 29 Working Party has given an Opinion[3] in February 2014 in the form of a 'referential' on EU BCRs (Binding Corporate Rules) and APEC's CBPRs, which

> does not aim at achieving mutual recognition of both systems. However, it could serve as a basis for **double certification.** In any case, data protection policies of applicant international companies operating both in the EU and the APEC areas **have to be approved respectively** by the relevant bodies in the EU Member States and in the APEC Economies, in accordance with the applicable approval procedures' (emphasis in original).

For each of 27 separate 'essential principles and requirements' of BCRs and/or CBPR, the referential lists both a 'common block' of elements which are 'common or similar' to the two, and 'additional blocks' of differences between the two or additional elements specific to each. The starting point for an assessment is that 26 of the 27 'essential principles and requirements' have 'additional elements' listed. In number 27 there is complete unanimity that an organisation's privacy rules must specify their effective date. In almost all of the other 26, the text of the additional elements is longer than the 'common block', in most cases far longer. In principles 9 and 11 they are roughly of equal length. In most cases it is the EU's additional requirements that are longer. In some cases there is no 'common block' at all, such as the very significant number 4, 'Requirements for data subjects and third party beneficiary rights'. While it is obviously necessary to read the 62 pages of the referential to gain a proper impression of how significant these differences are, it is beyond doubt that there are such wide differences that a lengthy period of study is required even to understand them, let alone build bridges to overcome them.

It therefore comes as a considerable surprise to read a report by authors from a consultancy firm, funded by Google, that reaches the reassuring conclusion[4]

---

[1] Graham Greenleaf, 'Five Years of the APEC Privacy Framework: Failure or Promise?', (2009) 25 *Computer Law & Security Report*, pt. 6 'Cross-Border Privacy Rules (CBPR) and the 'Pathfinders', <http://ssrn.com/abstract=2022907>.

[2] The Wikipedia 'House of cards' entry notes that 'it is also an expression that dates back to 1645 meaning a structure or argument built on a shaky foundation or one that will collapse if a necessary (but possibly overlooked or unappreciated) element is removed.'

[3] Article 29 Working Party *Opinion 02/2014 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* (European Commission, Article 29 Working Party, 28 February 2014) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf>.

[4] Malcolm Crompton, Annelies Moens and Chong Shao *Towards a Truly Global Framework for Personal Information Transfers: Comparison and Assessment of EU BCR and APEC CBPR Systems* (Information Integrity Solutions, September 2013).

> '…that operationally, BCR and CBPR take slightly different pathways to achieve the same result of providing protection for individuals while facilitating the efficient transfer of personal information across borders.'

The report is a detailed comparison of the EU BCR and APEC CBPR systems, for which a convenient summary has also been published.[5] The report does not ignore some major differences between the two systems, such as the EU's requirements that individuals have legal rights of enforcement through third-party beneficiary rights, and that there must be a single point of enforcement, and is worth reading for those and other points. However, it seems unjustifiably optimistic, when read against the Working Party's later Opinion, that these differences can be overcome, and a resulting global system for 'low friction cross-border transfers' (otherwise known as 'interoperability') can emerge based on something resembling APEC's CBPRs.

It should also be remembered that a BCR/CBPRs comparison is still only half the story in relation to transfers of personal data between EU and APEC countries, because the CBPRs is not restricted to intra-corporate transfers, but also aims to apply to inter-corporate transfers. The EU's equivalent instrument for inter-corporate transfers to countries which do not have laws considered 'adequate', is the EU Standard Contractual Clauses (SCCs). A SCC/CBPRs 'referential' would therefore also be needed, before any journey to full 'interoperability' could commence.

These detailed studies, seemingly coming from two different planets, make clear is that it is necessary for businesses and their advisers to obtain a very clear and detailed understanding of what APEC CBPRs does and does not do, and the foundations on which it is built. A summary follows.

Before proceeding to that summary, it is also worth noting that the APEC Privacy Framework (as distinct from the CBPRs) is only a voluntary agreement, it does not have any of the legally binding nature, or enforceability mechanisms, of either the EU Directive or even the Council of Europe data protection Convention. Also, its data privacy principles are considerably weaker than either of the European instruments, being roughly equivalent to the 1980 version of the OECD Guidelines.[6] Those two factors explain to a large extent why the gaps exposed by the Article 29 WP 'referential' are so wide.

How does APEC CBPRs work?

From its official documentation,[7] the proposed operation of the CBPRs may be summarised in twelve points.

1. An APEC economy must first have 'laws and regulations … the enforcement of which have the effect of protecting personal information consistent with the APEC Privacy Framework' to be able to participate in the APEC Cross-border Privacy Enforcement Arrangement (CPEA), an organisation of Privacy Enforcement Authorities (PEAs).[8] No independent body

---

[5] Laura Linkomes 'In search of a global framework for international data transfers' (2014) 127 *Privacy Laws and Business International Report*, pgs 8-9.

[6] See Greenleaf, 'Five Years of the APEC Privacy Framework'.

[7] See both: (i) APEC Electronic Commerce Steering Group (ECSG), 'Cross-Border Privacy Rules (CBPR)' <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx>; including CBPR Joint Oversight Panel Protocols; CBPR Policies, Rules and Guidelines; CBPR Intake Questionnaire; CBPR Program Requirements; Accountability Agent Application for APEC recognition; Template Notice of Intent to Participate; Cross Border Privacy Enforcement Arrangement. (ii) Cross Border Privacy Rules System (CBPRs) website < http://www.cbprs.org/>, including tracking of new developments, and 'Privacy in the APEC region',

[8] 'A PE Authority is any public body that is responsible for enforcing information Privacy Law, and that has powers to conduct investigations or pursue enforcement proceedings. It can be a national or sub-national authority. 'Privacy Law' is defined in the CPEA as the laws and regulations of an APEC economy, the enforcement of which have the effect of protecting personal information consistent with the APEC Privacy Framework.': *CPEA Fact Sheet.*

decides that the economy really does have the required law, it effectively 'self-assesses' that it does. Also, 'consistent with' does not imply enforcement of the whole Framework. (CORRECTION: As noted in the second article in this series, this paragraph '*should have stated the JOP does issue Findings Reports on each economy's application (as discussed in the above article). The point being made was the shortcomings of such JOP assessment, but it could be read as implying there was no JOP report.'*)

2. A Privacy Enforcement Authority (PEA) (a 'public body that is responsible for enforcing information Privacy Law, and that has powers to conduct investigations or pursue enforcement proceedings') from the APEC economy, notifies the CPEA Administrators of its intention to participate in the CPEA, and provide information confirming its powers etc. However, there is no independent assessment that the PEA really does have the required powers, it effectively 'self-assesses' that it does.

3. A 'Designated APEC government delegate' in the APEC economy informs APEC's Electronic Commerce Steering Group (ECSG) of its intent to participate in the CBPR; that it has a PEA that is participating in the CPEA; and that it intends to appoint an Accountability Agent (AA).

4. An applicant to be an Accountability Agent (AA) from the economy concerned (or subject to its jurisdiction) applies to CBPR's Joint Oversight Panel (JOP), submitting details of how it meets the Accountability Agent Recognition Criteria, and 'demonstrating' how it will meet CBPR Program Requirements in assessing companies applying for certification, monitoring compliance by them and dealing with complaints against them. The JOP does not actively investigate whether the AA applicant really does do what it claims.[9]

5. The JOP makes a recommendation for approval of the AA application to the 'APEC member economies', which means the decision is by those economies whose representatives participate in the meeting of the APEC Privacy Sub-group where the matter is on the agenda. Only some economies attend such meetings. The AA approval is only for one year, with re-application required annually.

6. The AA, once approved, may accept applications from companies within the jurisdiction of the economy from which they come, to certify that those companies comply with the requirements of the CBPR system, but only in relation to personal data 'that they have collected or received that is subject to cross-border transfer to other participating APEC economies'.[10] APEC CBPR does not apply to any other data held by a company, though they are 'encouraged' to apply the same company policies to it.[11] There is no CBPR mechanism for consumers to know whether particular items of their personal information fall within the 'subject to export' qualifying criterion.

7. The AA is to 'verify' an applicant company's self-certification of the compliance of its policies with the AA's programme requirements. The company's policies are to be regarded as confidential by the AA. There is therefore no mechanism by which external parties can assess either before or after certification whether a company has accurately stated its policies in order to obtain certification. Complaints can only be made in individual cases about non-compliance with CBPR requirements.

---

[9] See the discussion of the TRUSTe application in Part 2 of the article.

[10] *APEC CBPR System – Policies, Rules and Guidelines* (APEC, undated), p.3.

[11] *APEC CBPR System – Policies, Rules and Guidelines* (APEC, undated), p.3, fn. 10.

8. CBPR certification does not change a company's obligations to comply with all local legal requirements in the economy in which it is located.[12] In particular, any local restrictions on exports of personal data still apply.

9. The AA does not certify that the company complies with local data privacy laws of the economy concerned, only with its CBPR requirements,[13] which will often be lower. So a consumer cannot know if a CBPR-compliant company is in fact 'law abiding'. However, CBPRs participation does not relieve companies from complying with local data privacy laws.

10. An AA is required to investigate complaints made to it against a company it has certified, and to remove the certification of companies that fail to remedy breaches of the programme requirements within a reasonable time. The AA is required to refer a breach which has not been remedied in a reasonable time to an appropriate PEA 'so long as such failure to comply can be reasonably believed to be a violation of applicable law',[14] which leaves considerable discretion to the AA. An AA is not required to have the ability to impose financial penalties on companies in breach,[15] and there is no requirement to be able to award compensation to consumers. Therefore, the only additional remedy that the CBPRs offers consumers is that a company might have its certification removed.

11. AAs are required to 'release anonymised case notes ('on a selection of resolved complaints illustrating typical or significant interpretations and notable outcomes') and complaint statistics'.[16] This transparency, if made effective,[17] could be a strong point of APEC-CBPRs.

12. CBPRs only applies to controllers at present, but discussions continue concerning extension to processors.[18]

The limited effect of CBPR certification on a company

Companies considering the business case for CBPR accreditation (with its attendant and ongoing costs) need to appreciate how limited are the effects of being accredited by an AA.

(i) Certification only means that the company, in relation to its operations in one APEC economy, will deal with personal information it receives in accordance with the APEC Framework.

(ii) Such certification has no effect on the same company in its operations in other APEC economies. It would need to be obtained separately in each country to which data was to be transferred.

---

[12] *APEC CBPR System – Policies, Rules and Guidelines* (APEC, undated), p.10.

[13] *APEC CBPR System – Policies, Rules and Guidelines* (APEC, undated), p.11.

[14] *APEC Accountability Agent Recognition Criteria* (APEC, undated), criterion 14.

[15] JOP determination of TRUSTe AA application, 2013.

[16] *APEC CBPR System – Policies, Rules and Guidelines* (APEC, undated), p.15; *APEC Accountability Agent Recognition Criteria* (APEC, undated), criteria 10(g) and 10(h).

[17] APEC's JOP initially agreed to allow TRUSTe to publish statistics on larger sets of data, not only APEC-related complaints, which would have 'buried' the APEC data. After criticisms from civil society organisations, they reversed this: APEC CBPRs JOP 'Recommendation Report on APEC Recognition of TRUSTe' (JOP, 18 June 2013), pgs. 15-16.

[18] Nigel Waters 'APEC Cross Border Privacy Rules system awaits final component' (Privacy International, 5 March 2013) <https://www.privacyinternational.org/blog/apec-cross-border-privacy-rules-system-awaits-final-component> accessed 14 January 2014.

(iii) Certification does not in itself mean that personal data can be transferred from any other APEC economy. The law in each other economy must permit such transfers. At this stage no laws in APEC economies clearly provide that exports to APEC CBPR-compliant companies are allowed.

(iv) There is not, and will not be, any such thing as 'APEC-wide' certifications allowing companies to receive information from any APEC economy. This would require the laws in all 21 APEC economies to allow such transfers. If such transfers are not prohibited under existing laws, then APEC certification adds nothing.

(v) For the same reasons, APEC CBPR certification cannot have any direct effect on the ability of companies to import personal data from countries outside APEC.

(vi) As yet, there is no 'mutual recognition' or 'interoperability' of CBPRs certification by regional organisations outside APEC, such as the EU. Any notion of full 'interoperability' with EU Binding Corporate Rules (BCRs) is illusory[19], and partial consistency so as to reduce the paperwork in obtaining 'double certification' under both EU and APEC systems is the best that is likely to be achieved.[20] To the extent that this occurs, it may make the CBPRs more attractive.

(vii) If a company is based in a country which already has a data privacy law that meets or exceeds the low standard of the APEC Privacy Framework, there should be no benefit to that company in obtaining CBPR certification.

The business case?

Given the complexity and the essentially 'multi-bilateral' nature of the APEC CBPR processes, any company considering applying for certification would need to think carefully about the business case (initial and ongoing annually) for certification (or possibly, multiple certifications), including whether CBPRs has any benefits for the customers of the business. One law firm's authors have concluded after examination that[21]

> '…there is doubt as to whether any implementation of the CBPR System in Australia would be successful. For Australian organisations, there appears to be no compelling reason to participate in a resource-intensive scheme that ultimately falls below the high-water mark set by the Privacy Act … As equally doubtful is the CBPR System's adoption in other jurisdictions in the broader Asia-Pacific region.'

Potential certification customers need to take a very careful look at some rather different messages such as[22]

> 'For unrestricted flow of personal information across borders while establishing meaningful protection by your customers, TRUSTe is your APEC endorsed, data privacy solution.'

Perhaps regulators such as the US FTC and the APEC CBPRs JOP also need to give some thought to how their system can reasonably be represented to businesses and consumers.

---

[19] Put very briefly, one reason is that the EU's Binding Corporate Rules (BCRs) are solely about intra-company transfers of data, whereas APEC's CBPRs is primarily about inter-company transfers of data (but can also be used intra-company). In the EU, Standard Contractual Clauses (SCCs) are used for inter-company transfers.

[20] Article 29 Working Party *Opinion 02/2014.*.

[21] Michael Burnett and Peter Leonard, Gilbert + Tobin Lawyers, *Privacy Law Bulletin* (Lexis-Nexis Australia), June 2013, pgs 128-30.

[22] TRUSTe website <http://www.truste.com/products-and-services/enterprise-privacy/apec-accountability> accessed 16 April 2014.

The second part of this article will examine how APEC CBPRs has operated to mid-2014, and whether it has anything of value to offer from a consumer's perspective. *Chris Connolly, Nigel Waters and Blair Stewart have provided valuable comments on earlier versions of this article. All responsibility for content remains solely with the author.*