UNSW Law & Justice Research Series

Global CBPRs: A Recipe for Failure?

Graham Greenleaf

[2022] *UNSWLRS* 54
(2022) 177 *Privacy Laws & Business International Report* 11-13.

UNSW Law & Justice
UNSW Sydney NSW 2052 Australia

E: LAW-Research@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

Global CBPRs: A recipe for failure?

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

(2022) 177 *Privacy Laws & Business International Report* 11-13

Global CBPRs: An announcement

A 'Global Cross-Border Privacy Rules Declaration' was announced on 21 April 2022 by the US Department of Commerce.[1] It stated that Canada, Japan, the Republic of Korea, the Philippines, Singapore, Chinese Taipei, and the US, as 'current economies participating in the APEC CBPR System', had established 'the Global CBPR Forum'. In fact these are seven of the nine 'economies' that have been approved to participate in APEC CBPRs,[2] with the absence of Mexico and Australia going unexplained.

The Declaration only establishes the Forum and declares that it has the objective to 'establish an international certification system based on the APEC Cross Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) Systems'. It contains various aspirational statements of which the most ambitious is that it will 'promote interoperability with other data protection and privacy frameworks.' It will hold meetings at least biannually.[3]

The 'global' nature is that it declares that 'Participation in the Global CBPR Forum is intended to be open, in principle, to those jurisdictions which accept the objectives and principles of the Global CBPR Forum as embodied in this Declaration,' and that 'decisions regarding future participation … should be made on the basis of a consensus of all members.'

A small page of Frequently Asked Questions (FAQs)[4] which adds some operational details of what is apparently a transition from the APEC CBPRs to this new system. 'The founding members of the Global CBPR Forum will consult with Accountability Agents and certified companies in the APEC Systems to formally transition operations from APEC to the Global CBPR Forum and will provide at least 30 days' notice to Accountability Agents.' 'All approved Accountability Agents and certified companies will automatically be recognized in the new Global CBPR Forum based on the same terms…'. All that is said about global expansion is that 'The Global CBPR Forum members welcome consultations with jurisdictions that accept [its] objectives …'. At this stage there are no announced procedures for additional economies/countries to 'participate', nor for companies to be certified.

There is no indication that 'Global CBPRs' will operate any differently than APEC CBPRs has done for the last decade, except that any country in the world, not just the 19 APEC economies, can apply to join.

Something that the Declaration and the FAQ concerning Global CBPRs does not make clear is the standard of data protection against which Global CBPRs compliance will be measured.

[1] U.S. Department of Commerce 'Global Cross-Border Privacy Rules Declaration' 21 April 2022 <https://www.commerce.gov/global-cross-border-privacy-rules-declaration>

[2] APEC CBPRs System < http://cbprs.org/>

[3] From April 26-28, 2022, in Hawaii a 'multi-stakeholder workshop' on "Global Cooperation on Privacy and the CBPR System: The Path Forward" was held in Hawaii. No details are available.

[4] U.S. Department of Commerce 'FAQs' <https://www.commerce.gov/sites/default/files/2022-04/Global-Cross-Border-Privacy-Rules-Declaration-FAQ.pdf>

APEC CBPRs compliance is measured against the APEC Privacy Framework,[5] which is in substance the same as the OECD Privacy Guidelines of 1980. The OECD Guidelines were modified in 2013[6] by the addition of principles requiring data breach notification, and a 'privacy management programme' (for demonstrable accountability),[7] but little else. They remain 'a bastion of low privacy standards', of little use to anyone.[8] The APEC Privacy Framework's modifications in 2015 suggest but do not require data breach notification, but do require a 'privacy management programme'.[9] Both the OECD Guidelines and the APEC Privacy Framework are essentially frozen at the standards of privacy principles developed in the 1980s, and ignore the global development since then of stronger data privacy principles by both international instruments (such as the GDPR and Convention 108+) and national laws in 157 jurisdictions. There is no indication that new principles will be developed for the Global CBPRs system, so we must assume that they will continue to use the APEC Privacy Framework – or possibly the OECD Guidelines.

It seems that the position is that 'APEC CBPRs is dead – long live Global CBPRs!'

APEC CBPRs: A decade of failure

The best guide to the possible future of Global CBPRs may be the decade-long history of APEC CBPRs.

Ten years after the USA was approved as the first economy to participate in APEC CBPRs, its vital statistics are as shown in the table below. While 9 of the 19 APEC 'member economies' have been approved to participate in APEC CBPRs, only 5 of the 9 have taken the one step that makes 'participation' meaningful, the appointment of an 'Accountability Agent' (AA) to certify companies operating in their jurisdiction as 'CBPRs compliant'.

Canada and Mexico, both approved to participate in 2014, have still not appointed an AA after seven years. Australia (2018) and Mexico (2019) have had some years to do so, but also have failed to do so. Korea appointed an AA in 2019, and Taiwan did so in 2021, but neither of these AAs have yet certified any companies as CBPRs-compliant.

That leaves three countries with a claim to meaningful participation in APEC CBPRs. Japan's AAs have certified 3 companies in 6 years; Singapore's have certified 6 companies in three years. The most obvious explanation for this under-performance is that Japanese or Singaporean businesses cannot see any persuasive business case for paying the certification fees and undertaking the administrative requirements necessary for certification, and then for renewals of certification. Why would they, when both countries have data privacy laws which require higher standards of compliance than the lower 'APEC Privacy Framework' standards on which APEC CBPRs compliance is based? There is no need for foreign companies to rely on APEC CBPRs to transfer personal data to Japan or Singapore, they can rely on the protections provided by the Japanese and Singaporean laws instead.

---

[5] APEC 'APEC Privacy Framework (2015)' <https://cbprs.blob.core.windows.net/files/2015%20APEC%20Privacy%20Framework.pdf>.

[6] OECD 'Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data' (1980, modified 2013) <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>

[7] Ibid; for both additions, see 'Part Three. Implementing Accountability'.

[8] G. Greenleaf 'It's Nearly 2020, so What Fate Awaits the 1980 OECD Privacy Guidelines? (A Background Paper for the 2019 OECD Privacy Guidelines Review)' (2019) 159 *Privacy Laws & Business International Report* 18-21, <https://ssrn.com/abstract=3405156>

[9] See APEC 'APEC Privacy Framework (2015)', para. [20]

That leaves the US, with 33 companies certified after ten years. The number is trivially small, given the size of the US economy, but at least there is a potential benefit to these companies because, in the absence of any comprehensive data privacy laws, they can attempt to rely on their APEC CBPRs certification in order to justify obtaining data exports.

APEC economy	Approved to join	Accountability Agent(s) appointed	No. of Cos certified
US	2012	2013	33
JAPAN	2014	2015	3
CANADA	2014	–	–
MEXICO	2014	–	–
KOREA	2016	2019	0
SINGAPORE	2017	2019	6
TAIWAN	2018	2021	0
AUSTRALIA	2018	–	–
PHILIPPINES	2019	–	–
OTHER 10 APEC members	N/A	–	–
TOTALS	**9**	**5**	**42**

Table: APEC-CBPRs 'participation' as at 1 May 2022[10]

Only three countries have explicitly recognized APEC CBPRs compliance as a legal basis for data exports to CBPRs-compliant companies. Japan did so in 2016, by Guidelines issued by the Personal Information Protection Commission (PIPC).[11] However, in order to obtain a

[10] Source: APEC CBPRs Compliance Directory 'CBPR System Directory' <http://cbprs.org/compliance-directory/> as at 1 May 2022.

[11] See 'An APEC CBPRs 'back door' in G. Greenleaf 'Questioning 'Adequacy' (Pt I) – Japan' (2017) 150 *Privacy Laws & Business International Report*, 1, 6-11 <https://ssrn.com/abstract=3096370>.; see also G. Greenleaf 'Japan Joins APEC-CBPRs: Does It Matter?' (2016) 144 Privacy Laws & Business International Report, 18-21 <https://ssrn.com/abstract=2964499>.

positive adequacy Decision from the EU, the PIPC issued Supplementary Rule (4) in 2018,[12] the effect of which was to exclude data sourced from the EU under an adequacy Decision from the scope of the CBPR 'Japanese back door'. In its adequacy Decision concerning Japan the European Commission made it clear that transfers based solely on CBPRs compliance 'are clearly of a lower level' than what Japan's law now required.[13] Regulation 10 of Singapore's *Personal Data Protection Regulations 2014* (PDPR) allows transfers from Singapore to CBPRs-certified companies (in other jurisdictions) as providing 'at least comparable' protection as Singapore's law.[14] The Office of the Privacy Commissioner for Bermuda allowed CBPRs-based transfers in 2021.[15]

Global CBPRs: Who will buy in?

These CBPRs systems require at least three types of parties to be convinced that there is a good case for their participation in the system.

First, countries have to be convinced that participation by companies based in their country will allow more 'free flow' of personal data to their country. Since almost of the 157 jurisdictions that already have data privacy laws have laws which provide higher standards than the APEC Privacy Framework (or OECD Guidelines), it is hard to see why CBPRs compliance by a few companies will result in more personal data being transferred to their countries. This is particularly so because 'CBPRs compliance' does not mean that a company is compliant with its own country's data export restrictions. Of course, the relatively few countries that do not have comprehensive data privacy laws (notably, the US) may conclude that CBPRs will allow more data to be transferred to their country.

In addition, more countries will need to have provisions in their laws, like Bermuda, Singapore or Japan (except for EU-sourced data), recognizing that transfers to CBPRs-compliant companies are legitimate exceptions to the data transfer restrictions in their laws. Otherwise, it does not matter how many companies are CBPRs-certified. With only three countries taking this step in relation to APEC CBPRs, there is a serious issue of whether more countries will want to do so for a global system. In addition, countries considering enacting such provisions will need to consider whether this may imperil their prospects of obtaining a positive EU adequacy Decision (in light of Japan's experience), or prevent them from acceding to Convention 108+.[16]

---

[12] PIPC (Japan) *Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU based on an Adequacy Decision,* 2018

[13] In APEC CBPRs 'the protections do not result from an arrangement binding the exporter and the importer in the context of their bilateral relationship and are clearly of a lower level than the one guaranteed by the combination of the APPI and the Supplementary Rules': para. [79] *Commission Implementing Decision of 23.1.2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information*

[14] Singapore 'APEC Cross Border Privacy Rules (CBPR) System' <https://www.imda.gov.sg/programme-listing/Cross-Border-Privacy-Rules-Certification>;

[15] PrivCom Bermuda 'PrivCom recognises APEC CBPR System as a certification mechanism for overseas data transfers' 2 March 2021 <https://www.privacy.bm/post/privcom-recognises-apec-cbpr-system-as-a-certification-mechanism-for-overseas-data-transfers>. See Bermuda's PIPA s. 15(4).

[16] Article 14 of Convention 108+ refers to 'a real and serious risk that the transfer to another Party, or from that other Party to a non-Party, would lead to circumventing the provisions of the Convention'. Whether legislation concerning CBPRs-based transfers might be an impediment to accession is beyond the scope of this article.

The system requires one or more Accountability Agents. Unless they are subsidized by government,[17] they will be private companies who need to find a profitable business case in the certification of CBPRs-compliant companies. The costs of establishing certification systems, of developing a market for such a product, and of convincing companies to pay annual costs of re-certification, will require a non-trivial number of companies wanting certification. As yet, there is no successful example of such a CBPRs certification business.

Finally, enough businesses in a country need to be convinced that there is a good case for their paying the fees charged for certification and re-certification, and the internal costs of the certification process. Any business will have to ask: 'will this make it easier for our company to import personal data, to an extent greater than compliance with local laws?' Otherwise, why is this cost justified?

Conclusions: Scaling up a turkey?

In short, there are many hurdles to be overcome if Global CBPRs is to succeed. The underlying problem is the low standard against which CBPRs compliance by companies is assessed. The laws of many countries will not allow personal data to be exported to companies that only meet such a low standard. As a result, countries cannot see much advantage in having their companies CBPRs-compliant, Accountability Agents cannot see a viable business being built on providing certifications, and companies cannot see a business case justifying the costs and efforts of obtaining certification. Some unsuccessful initiatives can be salvaged by 'scaling up', making them available to a wider audience where they might be more popular. But if the fundamentals are unsound, 'scaling up' is unlikely to succeed.

[17] Singapore's IMDA says that companies may 'consider applying to Enterprise Singapore (ESG) to seek support for some of the costs for APEC CBPR certification and consultancy services' <https://www.imda.gov.sg/programme-listing/Cross-Border-Privacy-Rules-Certification> .