Privacy International Report on APEC Privacy developments, March 2011

*by Nigel Waters**

Cost-benefit case for the APEC CBPR remains elusive

2011 is supposed to be the year that the APEC pathfinder projects on Cross Border Privacy Rules (CBPR) deliver a functional system for businesses to be certified for transfer of personal information between participating APEC economies.

After the last round of APEC privacy meetings in Washington DC on 1-3 March, this prospect is looking increasingly remote. Even the basic set of documentation and processes required for the process of self-certification and assessment of businesses has yet to be fully agreed and endorsed, while discussion of the all-important governance and funding arrangements has not progressed far beyond where it had reached in mid 2010, which is not very far at all. All the hard questions about how the CBPR system will work in practice, and deliver the necessary level of confidence, have been shunted into this critical component (Project 8), with only one further round of face to face meetings left in 2011, in September in San Francisco.

The main reason for the lack of progress appears to be the failure of any governments or privacy regulators, apart from the US authorities, to seriously commit resources either for the necessary inter-sessional work on the Pathfinder, or for the longer term 'secretariat' functions that will be required in the operation of the CBPR system.

Of the seven privacy supervisory authorities in APEC economies, five of which are signatories to the Cross Border Privacy Enforcement Cooperation Arrangement (CPEA) established in 2010 as part of the CBPR system, only three attended the Washington meeting – the US Federal Trade Commission, the Canadian Privacy Commissioner's office and the newly established Mexican IFAI. The Australian, New Zealand, Hong Kong and Korean regulators were absent, although the first three have been regular contributors to inter-sessional work including the establishment of the CPEA. While there has been other inter-sessional drafting work, and periodic teleconferences, decisions can only be made at the six-monthly DPS meetings (and endorsed by the parent Electronic Commerce Steering Group (ECSG) which meets a few days later).

The critical CBPR governance issues can only be resolved when governments and the regulators declare their hand on what role they will play in the operation of the CBPR system, and commit resources.

In the meantime, there are disturbing signs that even before the CBPR system is settled and operational, business interests are already seeking variations and derogations from the

agreed processes. The International Chamber of Commerce (ICC) tabled a 'Sectoral Approaches' paper which makes a case for businesses that are already subject to other regulatory requirements (such as banking and financial services) to be exempted from at least some of the certification and assessment processes in order to become participants in the CBPR system. The Subgroup agreed to set up two working groups to explore concepts of mutual recognition and inter-operability, both for sectoral regulatory schemes and for existing trustmark or seal programmes, some of which are proposing to incorporate the CBPR obligations into their existing processes and programmes rather than administering them as a new programme.

However, there is as yet no commitment to proceed beyond some initial scoping discussion. it is unclear whether any 'mapping' of other processes or approvals to the CBPR requirements would be done in advance and confer automatic acceptance, or simply be a guide to assist Accountability Agents in assessing an application from a business which might wish to offer another approval as evidence of compliance, or to assist the CBPR governance body (as yet undefined) in assessing an applicant for Accountability Agent status.

The introduction of any inter-operability or mutual recognition processes, if they were subsequently developed, would inevitably complicate the practical implementation of the CBPR system and make it more difficult to explain and present the system, particularly to consumers. It may also make it more difficult for stakeholders in APEC economies to accept that the system has sufficient integrity. Business interests may find relatively weak governance acceptable (or even desirable?). But governments, privacy regulators and civil society are likely to have reservations about participation in the CBPR system as a basis for inter-jurisdictional transfers of personal information without certain assurances. These will need to include guarantees that the system includes rigorous, transparent and auditable assessments, not just of a business's assertions of compliance with the APEC Privacy Framework, but also of the independence, competence and credibility of Accountability Agents (AAs) and Enforcement Authorities (EAs).

Mere assertions by participating economies that their domestic AAs and EAs meet the CPBR system standards will clearly not be sufficient – given documented criticisms of various Trustmark schemes, of the EU-US Safe Harbor arrangement, and of the performance of some of the Privacy or Data Protection agencies. Some form of peer-review – currently envisaged as being by a Joint Operating Panel (JOP), will be necessary, but there is as yet no sign that anyone is going to step forward with the resources to establish such a body at even the minimum level required. It may be that in the long term a system of levies on participating businesses could fund the central infrastructure (even this has yet to be discussed seriously), but such a mechanism will not provide for the initial investment or 'bootstrapping' to establish a functional system from the outset.

All the stakeholders involved in the DPS discussions in Washington agree that the CBPR system will only work if it provides benefits to businesses that outweigh the costs of participation. Repeated re-assurances that the system will not undermine the requirement of any participant to comply with obligations under domestic laws, combined with the growing number of APEC economies with privacy laws imposing such obligations, mean that the stated objective of simplifying compliance requirements seems less achievable than ever. Set against the diminished benefit are the significant costs of participation – as yet unquantified but clearly rising as every new component of the system is finalised. These costs will need to be met either by APEC CBPR certified businesses and/or by participating economies' governments – although neither currently seems likely. The cost benefit case for businesses will be the focus of a seminar at the next Subgroup meeting in San Franciso in September. But at present, the cost-benefit case for the APEC CBPR remains as elusive as ever.

The Washington meetings also heard reports of developments in member economies, revealing a continuing trend towards domestic privacy legislation influenced as much by EU Directive and other instruments as by the APEC Privacy Framework.

Privacy International proposed a motion, adopted by the Subgroup and subsequently endorsed by the parent ECSG "that the DPS encourages member economies to support the participation of civil society in their economies in the development and implementation of privacy policies, consistent with the APEC privacy framework, both domestically and at the APEC level." This provides an opportunity for civil society in member economies, but they should not wait for invitations – they need to introduce themselves to the relevant policy-makers, making specific reference to the motion passed in Washington.

**Nigel Waters represents Privacy International at meetings of the APEC Data Privacy Subgroup. Some of the Washington meetings were also attended by Justin Brookman, Director of the Consumer Privacy Project at the US non-government organisation Center for Democracy and Technology (CDT).*