APEC Privacy Initiative

Report from representatives of civil society on meetings in Lima, Peru, 18-22 February 2008

Nigel Waters *Privacy International (PI)*
Philippa Lawson *Canadian Internet Policy and Public Interest Clinic (CIPPIC)*

Background

The meetings were held to progress implementation of the APEC Privacy Framework and Principles (adopted 2004), primarily at this time through the 9 'Pathfinder' projects agreed in 2007.

Relevant papers can be found (not always easily) on the APEC website at http://www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce.html - or http://aimp.apec.org/MDDB/pages/BrowseMeeting.aspx - browse February 2008 for the papers from the three Lima meetings.

Civil Society input

After a week of meetings (2-day seminar, 1 day workshop on the Pathfinder projects, and formal ECSG Data Privacy Subgroup meeting) there are grounds for cautious optimism. Both the direction of the initiative and the mood of participating economies appears to have moved towards meeting initial civil society concerns. These concerns are summarised in a paper presented and distributed by Nigel Waters at the seminar on 19 February (attached).

Philippa Lawson and Katitza Rodriguez representing the US *Electronic Privacy Information Centre (EPIC)* also made presentations at the Seminar (See Philippa's slides, attached). All three civil society representatives were slotted into panels on Outsourcing, but took the opportunity to make more general comments about the Framework and the Pathfinder. Philippa identified specific consumer concerns with outsourcing, and noted ways in which the APEC Privacy Principles are deficient in addressing those concerns. She emphasised the need for higher standards (e.g., limits on retention, no exception to due diligence and responsibility under the accountability principle, notice requirements re: foreign outsourcing) and the potential value of the APEC process in improving cross-border enforcement of both legislation and self-regulatory standards.

Katitza emphasized civil society's preference for national data protection legislation with higher standards and effective enforcement mechanisms, to ensure accountability and compliance. She suggested that those countries without data privacy legislation should look to those APEC economies with privacy laws that are already widely seen as setting a high standard (e.g. Canada). However, compliance and enforcement mechanisms still need to be reinforced even in those countries with data privacy laws.

Effect on regional privacy protection

Civil society acknowledges that it is now formally stated in the meeting papers that there is no intention to undermine the requirement to comply with domestic privacy laws, some of which set higher or more specific standards than the APEC privacy principles, which should be seen as a minimum 'floor'. The civil society view is that the APEC principles are not sufficient to stand alone as the body of a law for any regional economy.

The existence of the APEC Privacy Framework and Pathfinder does not seem to be deterring economies from considering legislative options, with Peru, China, Thailand and the Philippines all reporting in Lima that they are well advanced with the introduction of an information privacy law. In fact, it appears that *lack* of data protection laws constitutes a trade barrier – e.g. Peru has put data protection law on the fast track in order to attract more call centre operations. Of course the content of those laws is critical, and we should be prepared to argue for higher standards in each country, as needed.

Continuing stakeholder consultation

There is a clear consensus, now also repeatedly stated, of the importance of stakeholder consultation, including with civil society, both at the international level and in domestic economies.

In this spirit, there was significant overt support, and no formal objection, to the applications for guest membership at the Privacy Subgroup from PI and EPIC. Nigel and Katitza were allowed by their respective national delegations to speak in support of their applications. A recommendation to accept went forward from the Subgroup to the ECSG which met on 24 February. Regrettably one economy is understood to have objected and because APEC operates on a consensus basis, neither application was approved.

The applications have been deferred until the next formal ECSG meeting in August, and further background has been requested on the applicants (PI and EPIC). Given APEC's focus on trade and economic growth, we are constantly advised that privacy should be presented as a consumer protection and trust issue rather than as a human rights/civil liberties, but while we recognise that APEC must necessarily focus on privacy as consumer protection, civil society cannot resile from its position that privacy protection is also about human rights. In particular, the transfer of personal data from the economic realm to the political realm is a genuine concern – no economy will give up its sovereign right to legislate for access to personal data held within its borders, and this must therefore be a relevant consideration for any other economy assessing the level of privacy protection. PI and EPIC will provide further information and await the August decision.

In the meantime, work on the Pathfinder projects will continue before the next meetings in Lima in August through telephone and Internet conferences, and the civil society representatives were invited to participate in these, even without formal guest status. There remain significant opportunities for civil society to influence the implementation of the APEC Framework in this way, and also through direct input to the position of the individual economy delegations. However, capacity and resources are a significant

constraint on civil society participation, and it remains uncertain whether, even where invited, we will be able to have effective input to the Pathfinder projects.

There is also recognition of the need for better communications, transparency and 'outreach', and a 'friends of the chair' group has been formed to address these issues. It is recognised that there are some semantic obstacles to understanding, even amongst native English speakers, let alone those with other first languages. Consideration will be given to finding an alternative to the term Cross Border Privacy Rules (CBPR) as this implies yet another set of substantive standards, whereas the main focus of the work is on mechanisms and infrastructure for the effective implementation of existing privacy 'rules' with the APEC principles as the minimum 'floor'.

The APEC Privacy Subgroup has increasingly recognised the need to take account of developments in other international fora, specifically the work of the OECD Working Party on Information Security and Privacy. Civil society representatives have consistently emphasised the need to also engage with the European Union, as the different approaches must ultimately be reconciled, and we have welcomed the initial APEC-EU officials meeting in Montreal in September 2007 and the commitment to at least annual meetings.

How will the APEC implementation scheme work?

Having obtained confirmation that the CPBR approach is only *one* way of implementing the APEC Privacy Framework (albeit currently the main focus of the Privacy Subgroup) it has become clearer that the practical implementation of the CBPR approach is intended to be as follows:

- A business seeking to participate will prepare a document setting out how it will comply with any applicable standards, and how it will deal with any complaints about breaches; i.e. a version of the privacy policy or privacy statements which are required by some domestic laws (and by APEC principle II). (In the Pathfinder this is known as 'self-assessment' – project 1) This self-assessment will be based on a standard set of questions, currently being drafted by TRUSTe with input from all participants.

- The document would be assessed by an 'accountability agent' which might be a regulatory agency or a 'trustmark' organisation. Private accountability agents (e.g., trustmarks) would be approved based on a separate trustmark assessment process, guidelines for which are project 2. TRUSTe has also provided a first draft of this document for review by participants.

- Project 3 involves developing guidelines for trustmarks to use when assessing the compliance of organisations with the relevant legal/self-regulatory criteria.

- If assessed as meeting the requirements, the business would be included in a publicly accessible directory of compliant organisations (project 4).

- Regulators will establish mechanisms for cooperation on complaints that involve multiple jurisdictions (projects 5-7).

- Pathfinder project 9 will seek to test the entire process, starting with a number of volunteer businesses submitting self-assessment results documents for 'processing' by accountability agents. The complaints and enforcement mechanisms being developed in projects 6 & 7 will then be tested on hypothetical 'breach' scenarios. A number of US corporations, and TRUSTe have already volunteered, but the Subgroup is seeking a wider group for project 9. This is important given the current preference of Mexico, Japan, Vietnam and a number of other Asian member economies for a trustmark based approach.

Benefits of the approach, but some outstanding questions

The scheme would appear to offer the advantage of having businesses conduct a level of self-assessment which goes well beyond what is required by most domestic privacy laws, which are almost all complaint based, with a default untested assumption that data controllers are complying with the law. From draft assessment criteria presented in the 21 February workshop, the level of detail provided to 'accountability agents' would also exceed even that required by those European laws which require registration by data controllers. A crucial unanswered question is whether the self assessment details would be made public, or whether a participating business could provide a lesser level of detail in its public privacy notices, statements or policies. We will argue for the former.

Another important element currently missing from the Pathfinder is the mechanism by which the regulator in any one jurisdiction, or collectively, would assess the credentials of the 'accountability agent' in another jurisdiction. Project 2 will deliver assessment criteria for trustmarks, but who will make the decision that a trustmark scheme (or a regulatory agency) meets these criteria? As with organisational assessments, we will argue for full transparency with respect to trustmark assessments.

If the APEC Framework is to achieve its objective of removing barriers to the cross border flows of personal information, there is no escaping from the need, ultimately, for an 'adequacy assessment' mechanism similar to the EU Directive's Article 29 & 31 Committee processes. No economy, and in particular no regulator in those economies with a legislated cross border transfer principle (currently Australia, Canada, Hong Kong and New Zealand) will be able to avoid making a decision about which other jurisdictions meet their required minimum standards - both of substantive rules/principles, and of compliance and enforcement mechanisms. There is reluctance on the part of some participants to acknowledge this fact; indeed some participants seem to view the Pathfinder project as a replacement for traditional "adequacy" determinations, via a sort of "safe harbour" approach, although it is not clear how this can be reconciled with their acceptance of domestic legislative requirements..

It will be important, in our view, to ensure that the APEC assessment guidelines for both organisations and trustmarks meet our minimum standards. This will require a

significant expenditure of time and expertise on the part of civil society representatives. If APEC is serious about consultation with civil society, it needs to address the question of funding for continued participation by informed consumer and privacy advocates in the APEC processes.

Attachments

- A civil society perspective on the current work of the APEC Data Privacy Subgroup, Nigel Waters, PI (next section in this document and at http://aimp.apec.org/Documents/2008/ECSG/SEM1/08_ecsg_sem1_020.doc)
- Outsourcing: A Citizen/Consumer perspective – Philippa Lawson CIPPIC (Powerpoint presentation at http://aimp.apec.org/Documents/2008/ECSG/SEM1/08_ecsg_sem1_014.pdf)

Nigel Waters: nigelwaters@iprimus.com.au
Privacy International: http://www.privacyinternational.org
CIPCC: http://www.cippic.ca/en/

APEC Technical Assistance Seminar on International Implementation of the APEC Privacy Framework

Lima, Peru

19 February 2008

A civil society perspective on the current work of the APEC Data Privacy Subgroup, including the Data Privacy Pathfinder projects

Speaking notes from Nigel Waters, Privacy International

Objectives and role for a CBPR approach

- The objective of the APEC Framework is to ensure *effective and enforceable* privacy protection to facilitate cross border data transfers.
- Civil society remains unclear about the value of the Cross Border Privacy Rules (CBPR) approach in meeting this objective, given that is has been accepted that any overall scheme must meet the standards required by domestic regulation.
- This means that any CBPR scheme, which may include a trustmark element, must be able to guarantee enforceable remedies for breaches of the APEC principles in every participating economy, and this in turn will require legislative support (not necessarily a privacy law – could be in general consumer protection law).
- It is still not clear how CBPR mechanisms will assist businesses seeking to transfer personal data to or from jurisdictions which have minimum binding requirements. Greater clarity about what CBPR would look like, with examples, is urgently required.

Emphasis within the Pathfinder

- Given these reservations, civil society believes there is too great an emphasis in the Pathfinder on the CBPR approach, which is *only one* mechanism for implementation of the APEC Framework.
- Four of the Pathfinder projects (Nos 5,6, 7 & 8) are or can be independent of CBPR and support *all* implementation mechanisms. NGOs would like to see more emphasis within the Pathfinder on these projects.
- Civil society would also like to see the APEC Data Privacy Subgroup continue to explore and promote other ways of implementing the APEC Framework, with a preference for strong comprehensive information privacy laws as the simplest and least cost route both for consumers and for business.

Alternative models and legislative standards

- The APEC principles provide only a common minimum 'floor'. Many economies will choose to legislate a higher or more specific standards and civil society will support this.

- The choice is not just between the APEC principles and European models of regulation. Existing Asia-Pacific laws, such as those in Canada, Japan, Korea, Australia, New Zealand and Hong Kong also offer models which can operate within the APEC Framework whilst also potentially satisfy European standards – as Canada's private sector law already does.
- There is more difference in interpretations of the same principles by different regulators than there is between the different sets of principles (e.g. APEC and EU). This will be a challenge for the future, as cross-border enforcement co-operation will expose differences in interpretation.
- The CBPR approach, which may include a role for trustmarks, may complement other mechanisms and may provide some privacy protection for individuals in those economies in early stages of developing a regulatory response.
- Civil society is prepared to participate constructively in the development of the CBPR approach, provided it is not used as an excuse for rejecting alternative approaches to implementation such as legislation.
- Early attention needs to be given to the mechanisms and criteria for 'accreditation' of CBPRs and trustmarks, to demonstrate how they would comply with the requirements of those economies which have binding privacy regulation.

Stakeholder Consultation

- Civil society supports continued consultation with the privacy agencies (through the Asia Pacfic Privacy Agencies forum) and with the OECD, but also with European Data Protection agencies, since the APEC framework will eventually need to be reconciled with the 'adequacy' provisions of the EU Data Protection Directive.
- Civil society remains concerned about the imbalance of membership of the Data Privacy Subgroup, with no independent consumer voice to balance those of business interests.
- Civil society also calls on all member economies to implement the commitment in the Pathfinder to consultation with the full range of stakeholders in their own jurisdiction.

An alternative?

- Businesses may also wish to consider an easier solution than developing and implementing a complex CPBR approach – that is to adopt the highest common standards from all jurisdictions with binding privacy law, and then join with civil society in lobbying for all economies to legislate to this common standard. This would ensure that no business would suffer competitive disadvantage, whilst maximizing consistency and simplicity, in the interests of consumers and businesses alike.

Nigel Waters, nigelwaters@iprimus.com.au
Privacy International www.privacyinternational.org