The Public Voice Civil Society Meeting: "Next Generation Privacy Challenges and Opportunities"

Monday, 25 October 2010, Jerusalem, Israel

Panel Session: Establishing International Frameworks for Privacy Protection

Even with the celebration of the 30th Anniversary of the OECD Privacy Guidelines, there is growing interest in an international framework for privacy protection that would help ensure the enforcement of fundamental privacy rights. This panel will review the various frameworks for privacy protection, and explore the various new opportunities, including an "Umbrella Agreement" and further accession to Council of Europe Convention 108. This panel will also explore privacy issues in developing countries.

Panellist: **Nigel Waters**, Australian Privacy Foundation and Privacy International

Mixed motives and significant risks in the search for a new consensus

Current discussion of new or improved international privacy instruments is taking place in many different forums (OECD, EU, CoE, APEC, ICDPPC Madrid Resolution, Galway/Paris Accountability project, ISO). This discussion is generally healthy, but there are some significant risks:

- Consultation fatigue – all interested parties have limited resources for input, currently spread too thinly, with the risk of missing out on important discussions.
- Forum shopping by interested parties – if they don't get what they want from one forum, they can try another – we are all guilty of this, but it is not very efficient!
- Focus on private sector in some discussions may result in instruments which let the public sector 'off the hook'?
    - We need to resist any suggestion that either private or public sectors are the dominant risk to privacy – both are critical but in different ways. Also, the sectoral boundaries are increasingly blurred – government services are increasingly delivered by the private sector and governments seek access to private sector data for surveillance and enforcement.

We need to be clear about the objectives of the international discussions. Positive objectives and motives include:

- Greater clarity and certainty for data users and data subjects about rights and obligations
- Reduced bureaucracy and compliance costs
- Greater cross-border enforcement co-operation
- Easier, cheaper and quicker access to remedies in the event of breaches of rules

But there is also a less noble, but clearly evident objective - to accommodate less rigorous rules (principles) and/or lower standards of compliance, without allowing these differences to be used a non-tariff trade barrier. If this objective is realized, it will mean the re-emergence of 'data havens' where personal information can be processed in ways that would not be permissible in other jurisdictions.

A strong component of many international discussions is a greater emphasis on 'accountability' which, it is argued, can address the cross-border transfer dilemma by ensuring that a data user remains responsible for delivering its privacy promises wherever the data is processed. While superficially attractive, most of the accountability models currently being promoted do not overcome the reality of loss of effectively enforceable rights once personal information is transferred to a jurisdiction with lower standards or weaker enforcement mechanisms. However much cross border enforcement co-operation is improved, it cannot guarantee equivalent remedies and sanctions, and most accountability models inevitably involve a significant measure of self-regulation by data users, relying on a level of

trust and confidence which consumers and citizens are reluctant to grant = understandably in light of experience.

Civil Society input still limited and fragile

A strong Civil Society voice is arguably necessary because of the practical limitations in the ability of political and institutional systems (including privacy regulators) to represent the fundamental interests of consumers and citizens in the development of privacy law and policy.

Civil Society has at least gained a welcome place at the table in some forums recently (e.g. OECD CSISAC), but:

- Civil Society is still not formally recognized in other forums (e.g. APEC)
- Participation is not an end it itself - just because we are at the table doesn't necessarily mean that we are being listened to, or our views heard and understood
- There is a risk of being of being co-opted, with two potential outcomes:
    - Civil Society representatives may make undesirable concessions under pressure from a majority of other stakeholders
    - Other stakeholders are able to say that Civil Society has been consulted, even though they take no notice of our input, giving a false assurance.

Defending the universality of privacy protection

There is a risk that in all new discussions, there is an underlying presumption that it is privacy expectations and protection mechanisms that have to adapt to meet new 'realities', which include:

- in the private sector, that all new services and business models have to be accommodated, and
- in the public sector, that privacy must give way to security and efficiency imperatives
- in both sectors, that cross-border transfers are inevitable and must be accommodated.

Civil Society, in all jurisdictions and cultures, needs to re-assert key privacy principles as universal and non-negotiable. Some proposed services, business models and government surveillance and control initiatives will, bluntly, be unacceptable, as incompatible with inalienable privacy rights. This is not the same as saying that individuals have an absolute right to privacy, just that intrusions must always be justified, proportionate, limited etc.

Legitimacy of cross-border data transfer controls

Any international privacy instrument will need to address the issue of the required degree of similarity of laws to allow transfers between jurisdictions. Both the EU Directive and the Council of Europe Convention employ a test of 'adequacy', but this has fallen into disrepute largely because of the bureaucratic complexity of EU adequacy assessment and justified perceptions that the decisions that have been made have been arbitrary and inconsistent. This history should not however lead to the abandonment of the criterion. 'Adequacy', in the context of privacy protection, should not be a dirty word, and perhaps it is time to re-assert the legitimacy of 'Equivalence' as the preferred goal!

Civil Society must resist the suggestion that common high level principles can legitimately be interpreted in different ways in different jurisdictions, to accommodate so-called 'cultural differences'. This is not to deny the existence of some different perceptions and the need to take account of different political and business environments. The relative acceptability of national identity schemes in different jurisdictions is an example of such differences. But we must be constantly alert to spurious and self-serving attempts to use 'cultural differences' to accommodate lower standards of privacy protection.

Where jurisdictions exercise their sovereignty to apply lower standards of privacy protection for their own citizens, they must also accept the right of other jurisdictions to insist on higher standards to be maintained for any personal information involuntarily transferred (i.e. without the free and informed consent of the data subject). It will continue to be legitimate for international privacy instruments and domestic laws to include cross-border data transfer limitations to ensure no loss of protection.