APEC Data Privacy Seminar, Manila, 1 December 2011

Privacy Regulatory Models and the Consumer

Nigel Waters, Privacy International and the Australian Privacy Foundation[1]

Privacy is multi-faceted – personal (body), territorial (space), communications, and information. Focus in this seminar on the latter domain, but should not forget the others – need other protection tools/laws to deliver overall privacy rights.

Focus also on private sector and consumers, but also remember similar issues in public sector-citizen relationships (also private-public boundaries are increasingly blurred).

Most information privacy (data protection) regulation is derived from common source international instruments:

- OECD Guidelines (1980)
- Council of Europe Convention 108 (1981)
- EU Directive (1995)

All three currently under review

Newer initiatives include

- APEC Privacy Framework (2004-05)
    - Cross Border Privacy Rules system as a means of implementing the APEC Framework finalised in 2011 for commencement in 2012.
- International Commissioners' proposed international privacy standard (The Madrid Resolution, 2009)
- 'Accountability' project (private sector led but supported by various European Commissioners)

Often hear a simplistic analysis that there is a contest between a European and a US model of information privacy regulation, where the models are seen to have distinct characteristics:

European – comprehensive data protection legislation for both public and private sectors – detailed prescriptive rules – prior approval via registration/licensing – independent privacy specific regulator with significant powers (Data Protection Authorities or DPAs). Several other jurisdictions outside Europe have also adopted this model – particularly in Latin America, and Macau SAR.

US – sectoral laws as required – preference for more general, flexible rules – no prior approval – enforcement by sectoral regulators with other jurisdictions – greater role for self-regulation. Some Asian jurisdictions have adopted models arguably closer to this one e.g. Japan and Vietnam.

In reality, the environment is much more complex[2].

- EU principles leave much room for differential interpretation (and uncertainty).

[1] Nigel Waters represents Privacy International at international fora including the OECD and APEC privacy working groups, and is principal of Pacific Privacy Consulting www.pacificprivacy.com.au

[2] For a comprehensive review of privacy laws around the world, see Global Data Privacy in a Networked World by Professor Graham Greenleaf - http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1954296

- Some US sectoral laws are very prescriptive, and where regulators intervene, can do so more vigorously than European DPAs
- Self regulatory programmes can add a level of privacy awareness and compliance activity not guaranteed by the EU model
- Many jurisdictions outside Europe have adopted a 'third way' model – comprehensive laws with EU style principles, a strong DPA (at least on paper) but no prior approval, and a role for co-regulatory codes of practice (Australia, New Zealand, Canada, Hong Kong SAR, Mexico, and prospectively The Philippines and Thailand
- Others have chosen a different hybrid, such as Malaysia's new law (yet to be commenced). South Korea's law, revised in 2010, has moved decisively from the US towards the European model
- The role of individuals litigating to protect their own privacy varies significantly, with much more activity in the US than elsewhere, compensating to some extent for other perceived weaknesses
- The role of sectoral legislation varies – even in EU influenced or 'third way' jurisdictions, often specific privacy regulation (e.g. of direct marketing through Spam, Do Not Call laws)

Common themes/issues in all reviews and in development of newer initiatives

- Need for greater emphasis on practical compliance rather than procedural matters – on outcomes not process.
- Need for increased enforcement – perhaps involving new or increased powers for regulators
- Interest in enhanced role for intermediaries and trusted third parties
- Consideration of new rights – to anonymity, to be forgotten?
- Limitations of 'notice and consent' models
- New tools in regulatory toolkit, including
    - Data Breach Notification requirements (pioneered in the US where most States and Territories have enacted specific breach notification laws)
    - Privacy Impact Assessment
    - Privacy by design – early intervention
    - Representative complaints & class actions (super-complaints)
    - Statutory cause of action (in common law jurisdictions)

Civil Society favours most of these developments, but is wary of other potential 'losses' in the review/reform processes.

Risks, from a civil society perspective

- Strong lobbying by government agencies and corporations for greater flexibility – 'code' for accommodating new public administration and business models that involve greater surveillance, monitoring and data sharing (e.g. relaxation of credit reporting rules)
- Misuse of 'accountability' concept to promote self-regulation as a softer alternative with relief from supervision or sanctions (Accountability discussion OK as long as it is about *additional* obligations to 'demonstrate that you do what you say you are doing')
- Weakening of cross border data transfer rules to allow outsourcing/offshoring/cloud services on basis of assurances rather than enforceable jurisdiction
- Rearguard action by government agencies (and some business sectors) against application of universal principles – seeking exemptions or variation
- Authorisation of privacy intrusive initiatives under other laws (e.g. e-health, anti-money laundering, telecommunications interception, cybercrime, data retention) often co-opting private sector businesses as agents – although can often gain some privacy safeguards in legislation authorising intrusions