galexia

Asia-Pacific Region at the Privacy Crossroads (2008)

Chris Connolly, Galexia[1]

[1] Chris Connolly is a Director of Galexia, an independent consultancy specialising in privacy and electronic commerce. Research assistance for this article was provided by Steven Robertson and Amy Vierboom. <http://www.galexia.com.au>.

Web: www.galexia.com **Ph:** +612 9660 1111 **Fax:** +612 9660 7611
Post: Suite 95 Jones Bay Wharf, 26-32 Pirrama Road, Pyrmont NSW 2009, Australia

galexia

Document Control

Version

1.0

Date

25 August 2008

Source

The latest version of this article is available from
http://www.galexia.com/public/research/articles/research_articles-pa06.html

Copyright

galexia

Contents

1. Introduction

The Asia-Pacific region has reached a significant crossroads regarding the protection of privacy. This article examines current privacy developments in the Asia-Pacific region and provides some analysis of the benefits and risks of pursuing either the EU or the US/APEC approach to privacy regulation.

The region could choose to follow a path that is based on the traditional approach to privacy found in the EU *Data Protection Directive* of 1995[2] and the domestic laws of many countries, with strong comprehensive privacy legislation establishing independent regulators and imposing conditions on the transfer of personal information to parties in third countries. In this article it is referred to as the EU approach.

The alternative path is to follow a new model of privacy protection that involves greater reliance on self-regulation, self-certification, trust-marks and the registration of corporate rules. This approach is strongly advocated by US businesses and some features of this approach appear (in a limited way) in the APEC *Privacy Framework* of 2005[3] and related APEC Privacy Pathfinder Projects. In this article it is referred to as the US/APEC approach.

However, it is important to stress that the Asia-Pacific region does not face a *political* decision between the EU and APEC. It is more a pragmatic decision between the comprehensive privacy legislation favoured and encouraged by the EU, and alternative segmented business-centric approaches being promoted by US businesses and appearing in some aspects of the APEC Framework.

Note: This Article defines the Asia-Pacific region as East Asia, South East Asia and Oceania. It excludes South Asia (India, Pakistan etc.), Russia, and the Americas. The region covered by the countries included in this article is generically and commonly referred to as 'the Asia-Pacific region'.

2. Privacy regulation in the Asia-Pacific region

Many Asia-Pacific countries are members of regional groupings and are unlikely to develop privacy regulation without consideration of global and regional standards. Smaller countries in particular are careful to align their domestic regulations with regional and international developments.

The protection of privacy in the region is not uniform, although some clear trends are emerging. This section summarises the general approach being taken in each country (full details appear in *Appendix 1 – National Laws*).

Seven countries in the Asia-Pacific region have passed privacy legislation that is closely aligned with the broad EU approach. Four countries have draft legislation that is also closely aligned with the EU approach.[4]

Three countries have short privacy clauses in their e-commerce laws that could serve as a foundation for more detailed legislation in the future. This leaves five countries plus the majority of the small Pacific Island countries with no privacy legislation.

---

[2] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, 24 October 1995, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>.

[3] APEC Secretariat, *APEC Privacy Framework*, 2005, <http://www.apec.org/content/apec/publications/free_downloads/2005.html>.

[4] For recent legislative developments in the Asia-Pacific region, see Vierboom A, *Asia Pacific Privacy Developments 2007*, January 2008, <http://www.galexia.com/public/research/articles/research_articles-art48.html>.

Approach	Number of Countries	Countries
Privacy legislation	7	Australia, Hong Kong, Japan, Korea, Macau, New Zealand and Taiwan
Draft privacy legislation	4	China, Malaysia, the Philippines and Thailand
Privacy clause in e-commerce legislation	3	Indonesia, Vanuatu and Vietnam
No legislation	5+	Brunei, Cambodia, Laos, Myanmar and Singapore, plus the majority of the small Pacific Island countries.

The US/APEC approach has less traction in the region. Two countries have trust-mark schemes (Singapore and Japan), although these are effectively restrained to domestic companies. One further country is considering a trust-mark scheme (Vietnam).

One country in the region (Singapore) has adopted a policy of supporting privacy self-regulation rather than legislation, and has developed a Model Data Protection Code. However, this development was intended to be an interim measure on a longer path towards legislation, and Singapore is now considering privacy legislation.

Three countries (China, Malaysia, and the Philippines) have explicitly considered some of the APEC Privacy Framework Principles in the development of their draft legislation. However all three of these countries have chosen comprehensive EU style legislation rather than self-regulatory alternatives.

The dominant trend in the region therefore favours the development of EU style comprehensive legislation. It is important to note that in following the broad EU approach, countries in the Asia-Pacific region have chosen not to adopt exact copies of the EU Directive. For example, the former Hong Kong Privacy Commissioner described Hong Kong's privacy regime as 'European inspired but locally oriented, rather than simply a direct copy of what has gone before'.[5]

Privacy laws are also developing some unique characteristics in the Asia-Pacific region that are not based on developments in either the EU or the US. For example, privacy legislation in the region has been the subject of unexpectedly strong sanctions and enforcement.[6] Sanctions have included imprisonment, significant fines, substantial compensation payments and even orders to suspend business operations. This is in contrast to other jurisdictions, for example the US, where there has been no penalties or enforcement action under the specific provisions of the US Safe Harbour regime in its eight years of operation.

[5] Hong Kong Privacy Commissioner for Personal Data, *A View from Asia: Laying the Foundations for a Consolidated Approach towards Privacy to meet the Challenges ahead*, keynote address to the 4th IAPP Privacy and Data Security Summit and Expo, <http://www.pcpd.org.hk/english/files/infocentre/speech_20040219.pdf>.

[6] Connolly C, Lim YF, et al, *Privacy breach sanctions in the Asia-Pacific region*, July 2007, <http://www.galexia.com/public/research/articles/research_articles-art52.html>.

3. The EU approach

The key components of the approach established by the EU *Data Protection Directive* are that privacy regulation is comprehensive (covering the public sector and the entire private sector) and that regulation is contained in enforceable legislation. Typically the legislation will also establish an independent regulator.

Privacy legislation in the Asia-Pacific region (including the four draft bills) is closely aligned with the overall EU approach, with some minor exceptions. Legislation in Korea and Taiwan is not yet 'comprehensive' in that it only covers parts of the private sector. Also, legislation in Japan and Taiwan establishes multiple sectoral regulators, rather than a single independent regulator.

A further key element of the EU approach is that the legislation will place some conditions on the export of data to a party in a third country. These conditions vary in the Asia-Pacific region, but they are present in Australia, Japan, Korea, Macau, New Zealand and Taiwan. The Hong Kong legislation includes conditions, but these are not yet in force. All of the four countries with draft legislation include conditions in their drafts.

The general approach in the region is to allow the transfer of data to a third country that provides adequate protection. If the transfer is to a country without adequate protection, the legislation will still allow it to proceed subject to alternative conditions (such as explicit consent or protection via contract).

Note that in Japan and New Zealand the condition for transfer is that the original organisation remains responsible for the protection of privacy even where the information is transferred to a party in a third country (backed at least in Japan by an enforcement and penalty regime). This approach is similar to Canada (which was assessed as adequate by the EU in 2001).

The EU Directive is itself the subject of ongoing criticism and review. Key concerns include:

- There is a strong emphasis in the Directive on registration requirements such as notification (Articles 18 and 19) and publication (Article 21) – these can be overly bureaucratic and may distract attention and resources from managing privacy risks in more effective ways. The registration requirements appear to deliver little benefit and require considerable expenditure – they are the cause of significant concerns regarding compliance costs and are not present in privacy regulation in most other jurisdictions;
- The distinction between data controllers and data processors in the Directive is confusing and does not represent modern information practices; and
- The Directive does not cover law enforcement and security activities in an integrated way, resulting in a trend towards far reaching exemptions for law enforcement purposes without detailed justification.

In developing legislation in the Asia-Pacific region it has been common practice to ignore the more bureaucratic elements of the EU Directive. For example, the European experts advising China on their privacy legislation have specifically advised China not to include the registration requirements (Articles 18, 19 and 21) in their draft – noting that they are burdensome and expensive.[7] They also submit that these Articles are not required for the EU test of adequacy. Indeed, the EU assessed Canada's legislation as adequate despite the absence of registration requirements in Canada.[8]

[7] Sutton G, Xinbao Z, Hart T, *Personal Data Protection in Europe and China: What lessons to be Learned?*, EU-China Information Society Project, November 2007, <http://www.ucl.ac.uk/constitution-unit/foidp/downloads/Personal_Data_Protection_Public_CB_final_29_10_2007.pdf>.

Similarly, the development of draft privacy legislation in the Philippines began with a Bill that included registration requirements, but these are not expected to appear in the final legislation. Currently there are no jurisdictions in the Asia-Pacific region that repeat the registration requirements in the EU Directive.[9]

The result is that the Asia-Pacific region is free to accept the positive aspects of the EU approach while avoiding some of the more bureaucratic and expensive registration elements of the EU Directive.

4. The US/APEC approach

The aim of the *APEC Privacy Framework* 2005[10] is to promote a consistent approach to information privacy protection across APEC member economies. The history of the APEC Privacy Framework shows that it is in part a reaction to perceived problems with the EU approach. Interestingly, this development was not driven by consumer or civil society interests.

The key motivation for the development of the APEC Privacy Framework appears to stem from US business concerns regarding compliance with the EU Directive, and concerns regarding the potential expansion of the EU approach to other jurisdictions. These concerns coincided with growing interest in the US in the concept of enterprise-wide corporate privacy rules.[11]

Although this is not the sole motivating factor, and many other countries participated in the development of the APEC Privacy Framework, it is unlikely that the Framework would exist without the influence of US business interests.

For example, the Centre for Information Policy Leadership at US firm Hunton & Williams claims credit for the development of the APEC Privacy Framework:

> The Centre determined in 2001 that harmonised approaches to global data flows would be a significant issue for the business community, and began to research different approaches to data protection and privacy. In 2003 the Centre published a paper laying out a global framework for privacy and shared the paper with US government officials. The Centre and its members determined that APEC would be a good candidate for establishing a flexible alternative for global data flows. The Centre began participating in the APEC Privacy Subgroup in 2004. The APEC Ministers adopted the APEC Privacy Framework in November 2004. Today the Centre takes a lead role in pushing the activities that must be completed to move APEC implementation forward. Currently the Centre is pushing forward the development of instruments that would allow businesses to display their privacy platforms in a manner that matches the APEC principles.[12]

---

[8] *Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539)*, Canada, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002D0002:EN:NOT>

[9] Privacy legislation in Taiwan does contain some minor registration requirements for businesses. These requirements are the subject of proposed reforms in Taiwan.

[10] More information on the Framework and Principles is available at: <http://www.apec.org/content/apec/apec_groups/committees/committee_on_trade/electronic_commerce.html>.

[11] Wugmeister M, Retzer K, Rich C, *Global Solution For Cross-Border Data Transfers: Making The Case For Corporate Privacy Rules*, April 2007, <http://findarticles.com/p/articles/mi_qa4140/is_200704/ai_n19511009/>.

[12] The Centre for Information Policy Leadership, *APEC and Global Data Flows*, Hunton & Williams LLP, 2008, <http://www.hunton.com/Resources/Sites/general.aspx?id=325>.

One of the key US business concerns regarding the EU Directive is the legitimate criticism that the registration requirements in the EU Directive impose an onerous compliance burden, for little privacy benefit. However, there is no evidence that these registration requirements are being implemented in the Asia-Pacific region.

Other opposition from US businesses appears to be more ideological. For example, shortly after the EU Directive came into force, the Brookings Institute discussed the desirability of the EU assessing the adequacy of privacy protection in other jurisdictions:

> In essence, the Directive sets the EU up as judge and jury over the adequacy of privacy protections of other countries, including those of the United States. The extraterritorial ambitions of the EU understandably rankle many in the United States… The EU should recognise that various forms of 'self-regulation' that American firms and trade associations have been exploring can, if implemented, provide 'adequate' privacy protection.[13]

Over time this ideological opposition has mellowed. Three important factors now influence the relationship between the US and EU in this regard:

1. The EU Directive is first and foremost an attempt to protect the personal information of EU Citizens. Although this may have knock-on consequences for business, the key motivation is sound and the US recognised this in negotiating the US Safe Harbour Regime.

2. In turn, the EU has recognised that the protection of personal information in the US is fundamentally different to the EU, based as it is on a more litigious population exercising rights under consumer protection laws:

> When firms in this country [the US] hold out to the public that they are abiding by a privacy code and then fail to live up to that promise, they open themselves to legal challenge by the Federal Trade Commission and the states for engaging in an unfair trade practice, as well as to class action challenges for fraud and misrepresentation by private plaintiffs. In combination, these legal enforcement measures can provide every bit as much protection against privacy abuses as the formal legal machinery in the EU.[14]

3. In practice, concerns about the exercise of extra-territorial rights are ignored where there are pragmatic benefits to both the EU and the US (or US business interests). For example, the US has embraced the extra-territorial reach of the EU *Convention on Cybercrime*[15] and encourages countries in the Asia-Pacific region to join the Convention.

Despite the apparent resolution of major differences between the EU and the US regarding the protection of personal information on EU citizens, US business continues to express concern regarding the spread of the EU approach to other jurisdictions regarding non-EU citizens. Their main instrument for presenting an alternative approach to privacy protection is the APEC Privacy Framework.

The *APEC Privacy Framework* was published in 2004.[16] It is built around nine Privacy Principles, largely consistent with those of the 1980 OECD *Guidelines on the Protection of Privacy and the Transborder Flow of Personal Data*,[17] although with some minor differences.

---

[13] Litan R, *The European Union Privacy Directive*, Brookings Institution, 11 August 2008, <http://www.brookings.edu/testimony/1998/0507technology_litan.aspx>.

[14] Litan R, *The European Union Privacy Directive*; refer to footnote 13.

[15] Council of Europe, *Convention on Cybercrime*, CETS 185, signed 23 November 2001, entered into force 1 July 2004, <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

[16] More information on the Framework and principles is available at: <http://www.apec.org/content/apec/apec_groups/committees/committee_on_trade/electronic_commerce.html>.

There is ongoing debate about the extent to which the Principles either weaken or strengthen existing privacy principles found in instruments such as the EU Directive.[18] The latest view is that although there are many concerns regarding the implementation of the APEC Privacy Framework, the Principles themselves do not represent a significant departure from existing protections.[19] For the purposes of this Article only Principle 9 requires detailed analysis.

APEC Privacy Framework Principle 9 deals in a limited way with trans-border data flows:

> — **Principle 9 – Accountability**
> A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organisation, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organisation will protect the information consistently with these Principles.

This 'accountability' approach to cross-border privacy protection is consistent with the approach taken in Japan, New Zealand and Canada. It is also consistent with the approach recommended by the Australian Law Reform Commission (ALRC) in their review of Australian privacy legislation, although the ALRC has recommended retaining some additional conditions as alternatives to relying on accountability alone.[20]

The APEC Privacy Framework is complemented by a series of nine Pathfinder Projects. These were formally endorsed at the meeting of APEC Ministers in Sydney in September 2007.[21]

1. Self-assessment guidelines for business;

2. Trust-mark (accountability agent) guidelines;

3. Compliance review process of Cross-Border Privacy Rules (CBPRs);

4. Directories of compliant organisations;

5. Contact directories for data protection authorities and privacy contact officers within economies, as well as with accountability agents;

6. Templates for enforcement cooperation arrangements;

---

[17] Organisation for Economic Cooperation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980, <http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html> ('*OECD Guidelines*').

[18] Refer for example to Tan J, *A Comparative Study of the APEC Privacy Framework – A New Voice in the Data Protection Dialogue?*, 2008, Asian Journal of Comparative Law, vol 3 issue 1, <http://www.bepress.com/asjcl/vol3/iss1/art7/>; Greenleaf G, *The APEC privacy initiative: 'OECD Lite' for the Asia-Pacific?*, 2004, Privacy Laws and Business International Newsletter, issue 71, <http://www2.austlii.edu.au/~graham/publications/2004/APEC_V8article.html>; Greenleaf G, *Five years of the APEC Privacy Framework: Failure or promise?*, 2008, Asian Law Institute Conference (Singapore 2008); Pounder C, Why the APEC Privacy Framework is unlikely to protect privacy, Out-Law.com, 15 October 2007, <http://www.out-law.com/page-8550>; and Bennett C, *The APEC Privacy Framework: A Trading-Up of Standards or the Opposite?*, presented to the Conference on Privacy and Security, February 2006, <http://www.mser.gov.bc.ca/privacyaccess/Conferences/Feb2006/ConfPresentations/Bennett_Colin.pdf>.

[19] Waters N, *The APEC Asia-Pacific Privacy Initiative – a new route to effective data protection or a Trojan horse for self-regulation?*, June 2008, <http://www.pacificprivacy.com.au/NW APEC paper final.pdf>.

[20] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108, August 2008, chapter 31, <http://www.austlii.edu.au/au/other/alrc/publications/reports/108/31.html> ('*ALRC Report 108*').

[21] Full details of the Australian meetings regarding APEC are at <http://www.pmc.gov.au/privacy/apec/index.cfm>.

7. Templates for cross-border complaint handling forms;

8. Guidelines and procedures for responsive regulation in CBPR systems, and

9. A pilot program that can test and implement the results of the projects leading to the testing of a complete system.

A major, indeed dominant focus of the APEC work is now the development of Cross Border Privacy Rules. Cross Border Privacy Rules are described in detail below.

5. Other regional opportunities

Most countries in the Asia-Pacific belong to at least one of the three key regional organisations – APEC, ASEAN and the Pacific Islands Forum. Many countries also participate in specific regional meetings such as the East Asia Summit and the Asia-Europe Meeting (ASEM).[22] There may be opportunities outside the APEC Privacy Framework for the development of privacy protection in the region.

5.1. ASEAN Harmonisation

The Association of South East Asian Nations (ASEAN) has recognised that the absence of harmonised data protection legal infrastructure has the potential to become a barrier to cross-border trade and investment. Significant business opportunities in business process outsourcing may gravitate to jurisdictions with privacy protection that meet these requirements.

ASEAN has committed to the establishment of an integrated ASEAN Economic Community (AEC) by 2015. A significant target within this commitment is the development of a harmonised legal infrastructure for E-Commerce, as set out in the *Roadmap for Integration of e-ASEAN Sector*.[23]

The *Strategic Schedule for ASEAN Economic Community* contains the following specific target:

> Adopt the best practices / guidelines on other cyber law issues (i.e. data protection, consumer protection, Intellectual Property, ISP liability, etc.) to support regional e-commerce activities (2010-2013).[24]

As part of this plan, ASEAN may need to provide advice to Member Countries on the merits of the EU approach and the US/APEC approach to data protection.[25]

---

[22] <http://ec.europa.eu/external_relations/asem/intro/>

[23] *Roadmap for Integration of e-ASEAN Sector*, appendix to the *ASEAN Framework Agreement for the Integration of Priority Sectors*, November 2004, <http://www.aseansec.org/16689.htm>.

[24] ASEAN Secretariat, *Strategic Schedule for ASEAN Economic Community*, 2007, <http://www.aseansec.org/21161.pdf>. For an overview of responses to this target, see Connolly C, *Australian and regional regulatory responses to the key challenges of consumer protection in electronic commerce*, March 2008, <http://www.galexia.com/public/research/articles/research_articles-art51.html>.

[25] For an analysis of key issues in achieving regional harmonisation of data protection laws, see Connolly C, *Practical Issues in Achieving Regional Privacy Compliance*, presentation to the First Technical Assistance Seminar on the International Implementation of the APEC Privacy Framework, January 2007, <http://www.galexia.com/public/research/assets/apec_seminar_galexia_20070118.pdf>.

This plan may sound ambitious to outsiders, but ASEAN has a successful track record in implementing harmonised legal infrastructure in this field. For example, the *ASEAN Australia Development Cooperation Program (AADCP) – Electronic Commerce project*[26] helped ASEAN to implement harmonised e-commerce laws in eight Member Countries and draft laws in the remaining two Member Countries in just five years.[27]

5.2. Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

Another potential tool for privacy protection in the region is the Council of Europe *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*..[28] Although this is a European instrument it is open for signature by non-European countries. In 2008 the Convention's Consultative Committee recommended that non-member states, with data protection legislation should be allowed to accede to the Convention.[29]

Commentator Graham Greenleaf has noted some potential benefits of this approach for countries in the Asia-Pacific:

- Signing by one or more countries would encourage other Asia-Pacific countries to develop their laws and enforcement to the Convention standard;
- The Convention sets a standard higher than APEC, for example the Convention requires comprehensive laws and an independent authority;
- The Convention also requires data export limitations, including an 'adequacy' test (although this is contained in the additional protocol to the Convention,[30] which raises further complexities regarding implementation[31]).[32]

Again, this approach appears ambitious. But there are some precedents in the region. Although countries in the Asia-Pacific region have traditionally been slow to sign international instruments, there appears to be an exception for e-commerce related laws.

---

[26] Galexia, *Harmonisation of E-Commerce Legal Infrastructure in ASEAN*, April 2008, <http://www.galexia.com/public/research/articles/research_articles-art53.html>.

[27] Connolly C, *Harmonizing Cyber Legislation At The Regional Level: The Case Of ASEAN*, in United Nations Conference on Trade and Development, *Information Economy Report 2007–2008*, February 2008, <http://www.unctad.org/Templates/WebFlyer.asp?intItemID=4462&amp%3Blang=1>.

[28] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, CETS 108, signed 28 January 1981, entered into force 1 October 1985, <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>.

[29] Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [ETS No. 108], *Abridged report of the 24th meeting (Strasbourg, 13-14 March 2008)*, CM2008(81), 15 May 2008, <https://wcd.coe.int/ViewDoc.jsp?Ref=CM(2008)81>.

[30] Council of Europe, *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows*, CETS 181, signed 8 November 2001, entered into force 1 July 2004, <http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm>.

[31] Greenleaf G, *Non-European states may join European privacy convention*, August 2008, Privacy Laws and Business International issue 94, <http://www.privacylaws.com/>.

[32] Greenleaf G, *Asia-Pacific developments in information privacy law and its interpretation*, 30 March 2008, <http://law.bepress.com/cgi/viewcontent.cgi?article=1007&context=unswwps>. See also Greenleaf G, *Asia-Pacific developments in information privacy law and its interpretation*, presentation to the Privacy Issues Forum, 30 March 2008, <http://www.privacy.org.nz/assets/Files/74942725.ppt>.

The Council of Europe *Convention on Cybercrime*[33] has been adopted outside the EU, including adoption in the region by Japan. The Philippines are listed as an official observer to the *Convention on Cybercrime* and there is considerable interest in signing *Convention on Cybercrime* in Australia and Indonesia.

Similarly, the UN *Convention on the use of electronic communications in international contracts* only came into force in late 2006,[34] but it has already been signed by China, Korea, the Philippines and Singapore.

Signing the Council of Europe *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* could be an interesting alternative to achieving a regional standard of protection, although it does appear a 'long-shot' at this stage.

5.3. Asia Pacific Privacy Authorities (APPA)

Asia Pacific Privacy Authorities (APPA) is a regional forum for privacy regulators to meet and exchange ideas about privacy regulation, new technologies and the management of privacy enquiries and complaints. Members include national privacy regulators from Australia, Canada, Hong Kong, Korea, Macau, New Zealand and several smaller domestic privacy agencies.[35]

APPA is growing in importance as a regional privacy body and attracting new members. However, it is primarily a forum for the discussion of administrative issues between existing privacy regulators, and does not play a significant role in the promotion of new privacy regulation.

6. Emergence of a global privacy norm?

In establishing legislation to govern privacy issues relating to electronic data, the most prominent legal instruments remain the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* of 1980,[36] the EU *Data Protection Directive* of 1995,[37] and the APEC *Privacy Framework* of 2005.[38]

Of these instruments, an argument can be made that the EU approach to privacy protection is rapidly becoming the global norm. In the list of 'advanced economies' developed by the International Monetary Fund (IMF), 29 of the 31 economies have privacy legislation that is broadly aligned with the EU approach. Only the US and Singapore have a different approach to the protection of privacy (and even in the US many companies have joined the US Safe Harbour regime established to ensure compliance with the EU Directive).

---

[33] Council of Europe, *Convention on Cybercrime*, CETS 185, signed 23 November 2001, entered into force 1 July 2004, <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

[34] Ravindra P, *UN Convention on the use of Electronic Communications in International Contracts to come into force*, July 2006, <http://www.galexia.com/public/research/articles/research_articles-art41.html>.

[35] <http://www.privacy.gov.au/international/appa/>

[36] *OECD Guidelines*; refer to footnote 17.

[37] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, 24 October 1995, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>.

[38] *APEC Privacy Framework*; refer to footnote 3.

The following Table summarises the privacy approach taken by the 31 Advanced Economies recognised by the IMF.[39] Advanced Economies are modern market economies that have a high level of GDP per capita, but excludes countries that rely predominantly on a single source of income (e.g. oil reliant economies such as Brunei and Saudi Arabia).

	Country	Privacy Law	Coverage	EU Directive – Adequacy
1	Australia	The Privacy Act 1988	Comprehensive legislation	Awaiting assessment. Unlikely to be assessed as adequate while current exemptions for small business and employees remain in place. The Australian Law Reform Commission has recommended the removal of both exemptions.
2	Austria	Federal Act concerning the Protection of Personal Data 2000, (Datenschutzgesetz 2000 - DSG 2000)	Comprehensive legislation	EU Member
3	Belgium	Law of December 8, 1992 on Privacy Protection in relation to the Processing of Personal Data as modified by the law of December 11, 1998 implementing Directive 95/46/EC	Comprehensive legislation	EU Member
4	Canada	Personal Information Protection and Electronic Documents Act 2000 (PIPEDA)	Comprehensive legislation	Assessed as Adequate by EU on 20 December 2001[40]
5	Cyprus	Processing of Personal Data (Protection of the Individual) Law 138(I) 2001	Comprehensive legislation	EU Member
6	Denmark	Act on Processing of Personal Data (Act No. 429) 2000	Comprehensive legislation	EU Member
7	Finland	Personal Data Act (523/1999)	Comprehensive legislation	EU Member
8	France	Law 2004-801 of 6 August 2004 modifying law 78-17 of 6 January 1978 relating to the Protection of Data Subjects as Regards the Processing of Personal Data	Comprehensive legislation	EU Member
9	Germany	Federal Data Protection Act 2001 (Bundesdatenschutzgesetz - BDSG)	Comprehensive legislation	EU Member
10	Greece	Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data	Comprehensive legislation	EU Member
11	Hong Kong SAR	Personal Data (Privacy) Ordinance 1995	Comprehensive legislation	Unlikely to be assessed as adequate until trans-border data provisions come into force.
12	Iceland	Act on the Protection and Processing of Personal Data, No. 77/2000	Comprehensive legislation	European Free Trade Association (EFTA) Member
13	Ireland	Data Protection Act 1988	Comprehensive legislation	EU Member

[39] International Monetary Fund, *World Economic Outlook 2008: Country Composition of WEO Groups*, April 2008, <http://www.imf.org/external/pubs/ft/weo/2008/01/weodata/groups.htm>.

[40] *Commission Decision 2002/2/EC of 20.12.2001 on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act*, Official Journal L 2/13, 4 January.2002, <http://eur-lex.europa.eu/LexUriServ/site/en/oj/2002/l_002/l_00220020104en00130016.pdf>.

	Country	Privacy Law	Coverage	EU Directive – Adequacy
14	Israel	The Protection of Privacy Law 5741-1981, 1011 Laws of the State of Israel 128	Comprehensive legislation	Reforming laws as part of the EU assessment process. Likely to be assessed as adequate before 2010.
15	Italy	Italian Personal Data Protection Code (Legislative Decree no. 196 of 30 June 2003)	Comprehensive legislation	EU Member
16	Japan	Personal Information Protection Law 2003	Comprehensive legislation	Awaiting assessment. May be some concerns regarding adequacy of access to data provisions and exemption for small record holdings.
17	Korea	Act on the Protection of Personal Information Maintained by Public Agencies 1999 Act on Promotion of Information and Communications Network Utilization and Information Protection 2001	Partial legislation covering the government and parts of the private sector.	Proposed law reform in Korea may result in comprehensive private sector coverage, increasing prospects of an adequacy assessment.
18	Luxembourg	Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data	Comprehensive legislation	EU Member
19	Malta	Data Protection Act 2001 (Act XXVI of 2001)	Comprehensive legislation	EU Member
20	Netherlands	Personal Data Protection Act 2000 (Wet bescherming persoonsgegevens)	Comprehensive legislation	EU Member
21	New Zealand	The Privacy Act 1993	Comprehensive legislation	May be assessed as adequate once trans-border data provisions are strengthened. New Zealand commitment to amending law and seeking EU Adequacy assessment by 2011.
22	Norway	Personal Data Act 2000	Comprehensive legislation	European Free Trade Association (EFTA) Member
23	Portugal	Act on the Protection of Personal Data (Law 67/98 of 26 October), (*Lei da protecçao de dados pessoais*)	Comprehensive legislation	EU Member
24	Singapore			
25	Slovenia	Personal Data Protection Act 1999	Comprehensive legislation	EU Member
26	Spain	Organic law 15/99 of 13 December 1999 on the Protection of Personal Data, (*Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal*)	Comprehensive legislation	EU Member
27	Sweden	Personal Data Act 1998	Comprehensive legislation	EU Member
28	Switzerland	Federal Law on Data Protection 1992	Comprehensive legislation	Assessed as Adequate by EU on 26 July 2000[41]
29	Taiwan	Computer-Processed Personal Data Protection Law 1995	Partial legislation (covering some industry)	Proposed law reform in Taiwan may result in comprehensive private sector coverage, increasing prospects of an adequacy assessment.
30	United Kingdom	Data Protection Act 1998	Comprehensive legislation	EU Member

[41] *Commission Decision 2005/518/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland*, Official Journal L 215/1, 25 August 2000, <http://eur-lex.europa.eu/LexUriServ/site/en/oj/2000/l_215/l_21520000825en00010003.pdf>.

	Country	Privacy Law	Coverage	EU Directive – Adequacy
31	United States	International Safe Harbor Principles	Partial legislation (covering the public sector and some private sector organisations)	Safe Harbour regime covers US businesses who opt-in. Assessed as Adequate (for those businesses who comply) by EU on 26 July 2000.[42]

The Table shows that, at least for modern advanced economies, a clear global norm has developed for privacy protection, based on comprehensive legislation with conditions for the transfer of personal information to third countries. Singapore finds itself in perhaps an uncomfortable position as the only advanced economy on the list to have no privacy legislation at all.

7. Business Compliance

It is important to make an objective comparison between the business compliance requirements under the EU and US/APEC approaches.

A key motivating factor for the US/APEC approach is to simplify and streamline business compliance, in comparison with the perceived problems with the EU approach. For example, the Centre for Information Policy Leadership has stated:

> A growing number of multinational businesses, including members of the Center, have expressed increasing interest in emerging information privacy and security legal regimes in East Asia. This heightened attention reflects a concern that East Asian nations may follow the lead of European countries in developing restrictive privacy laws or a wide range of privacy laws that unnecessarily burden multinational information flows. At the same time, there is hope that, following upon the success of APEC in developing moderate privacy principles, East Asia might be the first region to develop harmonised, moderate privacy laws that facilitate multinational commerce, trade and travel.[43]

For domestic business compliance there is little difference. The APEC Privacy Framework requires compliance with domestic legislation, and as we have seen the domestic legislation in the Asia-Pacific region is very similar to that in the EU.

However, business compliance for cross-border information flows is more complex.

In the EU, business compliance for cross-border information flows requires consideration of Article 25 of the EU Directive, which places conditions on the transfer of the personal information outside the EU. In the US/APEC approach, Principle 9 – Accountability, must be considered.

[42] *Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce*, Official Journal L 215/7, 25 August 2000, <http://eur-lex.europa.eu/LexUriServ/site/en/oj/2000/l_215/l_21520000825en00070047.pdf>.

[43] The Center for Information Policy Leadership, *East Asia Privacy Leadership Project*, Hunton & Williams LLP, August 2005, <http://www.hunton.com/files/tbl_s10News/FileUpload44/11898/East_Asia_centerpiece.pdf>.

7.1. Business Compliance (EU)

Article 25 of the EU *Data Protection Directive* prohibits the transfer of data any country outside the EU, unless the country has been recognised as having an 'adequate' level of data protection in place. However, Article 26 lists several exceptions to this requirement:

> 1. …Member States shall provide that a transfer… to a third country which does not ensure an adequate level of protection… may take place on condition that:
>
> (a) the data subject has given his consent unambiguously to the proposed transfer; or
>
> (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or
>
> (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
>
> (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
>
> (e) the transfer is necessary in order to protect the vital interests of the data subject; or
>
> (f) the transfer is made from a [public] register…
>
> 2. … a Member State may authorise a transfer… to a third country which does not ensure an adequate level of protection… where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

Binding Corporate Rules (BCRs) are one mechanism for meeting the Article 26(2) exception, allowing an organisation (or corporate group) with operations in multiple countries (some of which are outside the EU and lack 'adequate' status) to transfer data across borders, but within the organisation. The European Union's Article 29 Data Protection Working Party publishes occasional guidance on the use of Binding Corporate Rules.

To date BCRs have had limited take-up. The approval process is complex and expensive, and approval may also be very restricted (for example, to human resources data only). In an effort to simplify and clarify the BCR approval process, the Working Party recently released a series of Working Documents setting out the requirements of a successful BCR application.[44]

However, these do not address the key difficulty in gaining approval for a BCR – BCRs must be approved by the data protection authority of every EU Member State out of which the organisation wishes to transfer data.

It is difficult to see any significant benefit offered by BCRs regarding business compliance. Their use is limited to situations where data is transferred within a corporate group, and the expense and complexity of the application process will deter many organisations.

[44] The Working Documents are available from the Article 29 Working Party: <http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm>.

Alternative means of business compliance are available that have less limitations and may ultimately be simpler and quicker to implement. These include the use of 'appropriate contractual clauses'. The European Commission issued a set of model contract terms to satisfy this requirement in 2001. An improved set of model contract terms (known as Set 2) came into force in April 2005. Further revisions and improvements are expected to be released in late 2008.

One concern with the model contract terms is that some Data Protection Authorities in the EU still require contracts to be filed with their office. Other EU countries require that the agreement is pre-approved by the local regulator before the transfer occurs (although if the model terms have been used this is a formality).[45]

Fortunately this 'registration' approach has not been followed in any Asia-Pacific jurisdiction, and even in Europe the number of jurisdictions requiring registration is falling.

The use of model contract terms seems highly preferable to the use of BCRs, and since the improvements to the model contract terms came into force in April 2005, it is difficult to identify any significant outstanding business concerns with the compliance requirements in the EU. Obviously the simplest form of compliance remains available – sending data to countries that have been assessed as adequate – and hopefully this list will grow over time.

7.2. Business Compliance (APEC)

Business compliance under the APEC Privacy Framework is complex. Domestic compliance is not affected at all – so the focus is on cross-border compliance.

Unlike the EU there is no mechanism in APEC for the provision of model contract terms as a mechanism to assist business compliance. During the early development of the APEC Privacy Framework there was some discussion of developing model contract terms, but this is no longer on the agenda.

The APEC focus is on the development and recognition of an organisation's Cross Border Privacy Rules (CBPRs). An organisation will prepare a draft privacy policy (their Cross Border Privacy Rules) that describe how they comply with privacy standards and how they manage complaints (Pathfinder Project 1 will provide a set of questions to assist in the development of this document).

These draft Cross Border Privacy Rules will be assessed by an approved accountability agent against a set of common criteria (the criteria are being developed in Pathfinder Project 3). The accountability agents will vary per jurisdiction – they could be Privacy Commissioners or perhaps trust-mark scheme operators. If an organisation's CBPRs are assessed as compliant they will be added to a public directory of compliant organisations.[46]

Cross Border Privacy Rules are proposed as a solution to a perceived compliance issue in the region:

> ...difficulties for companies in having to seek approval from different agencies in a number of economies for the same proposal for information flows.[47]

---

[45] Refer to Boschee K, *International Data Protection Law Restrictions On International Transfers Of Personal Data*, Faegre & Benson LLP, 2005, <http://www.acc.com/chapters/program/dallas/dataprotect.pdf>.

[46] Asia-Pacific Economic Cooperation, *The Cross-Border Privacy Rules – Implementation and Operating System*, 2006/SOM3/ECSG/DPM/009, September 2006, <http://www.rsaconference.com/uploadedFiles/2007/us/Conference_Content/ESAF/Cross_Border_Privacy_Rules_Implementation_and_Operation.pdf>.

[47] Peter Ford, *APEC Privacy Framework June 2005 Domestic Implementation*, 1-2 June 2005, <http://www.pcpd.org.hk/english/files/infocentre/1peterford1.pdf>.

The claimed benefit of CBPRs is that they will be 'recognised across APEC':

> A system that permits the wider use of CBPRs acknowledges that businesses already recognise that it is essential to protect the personal information of their customers. Developing a scheme that provides guidance on how CBPRs can meet the APEC-wide standards of the APEC Privacy Principles means that business CBPRs can be recognised across APEC economies.[48]

In practice, an organisation will possibly be listed on an APEC website as compliant, but it appears unclear what effect this has on individual jurisdictions. One US commentator has argued that each jurisdiction will then be bound to 'recognise' the organisation as compliant if it has been approved by any other jurisdiction:

> The rules must be approved by an accountability agent, and a national authority must submit the name of the approved entity to the APEC Secretariat to be posted to a Web site. Once a company's cross-border rules are approved by one economy, they must be recognised by all other participating economies.[49]

This seems to be a bizarre conclusion to reach, and it is not supported by any evidence in the Asia-Pacific region. No jurisdiction in the Asia-Pacific has an up-front registration requirement for an organisation's privacy policies. Each jurisdiction would currently only assess a privacy policy in relation to a complaint. In order for this to work, every jurisdiction would have to introduce new legislation providing regulators with an 'approval' or 'recognition' power (and the appropriate new resources to implement this) – this appears completely unnecessary and is not in keeping with the legislative approach taken in any Asia-Pacific jurisdiction.

Within APEC, there is also some recognition that Cross Border Privacy Rules may only be relevant for a small number of businesses:

> This arrangement will not be practicable for the vast majority of companies operating in APEC, but it is an option for leading global corporations to show their bona fides as 'good corporate citizens'.[50]

Perhaps the APEC CBPR approach is more closely aligned with trust-mark developments in the region. There is some interest in trust-marks in the Asia-Pacific and they are currently in use in Japan and Singapore (and proposed in Vietnam). Trust-mark schemes do include registration and pre-approval requirements.

However, great care should be taken before placing any reliance on trust-mark schemes as a form of cross-border privacy protection:

— In practice trust-mark schemes are effectively restrained to domestic companies. For example, trust-mark scheme information in Japan and Vietnam is largely available only in local languages. In Japan the list of trust-mark members is not available in English and the trust-mark logo itself is written in Japanese characters.

---

[48] <http://www.pmc.gov.au/privacy/apec/cross-border.cfm>

[49] Abrams M, *How does 'privacy' translate abroad?*, The National Law Journal, 31 March 2008, <http://www.hunton.com/files/tbl_s47Details/FileUpload265/2186/Abrams_How_Does_Privacy_Translate_Abroad.pdf>.

[50] Malcolm Crompton, *APEC Symposium on Information Privacy Protection in E-Government and E-Commerce*, 20-22 February 2006, <http://www.apec.org/apec/publications/all_publications/telecommunications.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/workinggroups/telwg/pubs/2006.Par.0012.File.v1.1>.

— Trust-mark schemes also tend to provide broader coverage than privacy – for example the Singapore trust-mark is a generic e-commerce trust mark, with only minor references to privacy.

— Trust-mark schemes have virtually no coverage beyond consumer-facing websites – they are simply not used for the majority of cross-border data transfers in the region.

— Trust-mark schemes have very little support from consumer and non-government organisations, primarily because voluntary trust-mark schemes have had no impact in any jurisdiction on the type of behaviour that causes consumer problems.

It is very difficult to see how trust-mark schemes can even begin to offer cross-border privacy protection in comparison with legislation, and it is surprising to see how much effort has gone into accommodating trust-mark schemes within the APEC Privacy Framework.

In the EU the Binding Corporate Rules are a pragmatic workaround for data being sent out of the EU, but within a corporate group. They have been rightly criticised as expensive and cumbersome. In APEC the CBPRs are more ambitious, but there is no guarantee it will be simpler or cheaper than the EU process.

Organisations still need to comply with local domestic requirements, including relevant conditions on transborder data flows. No jurisdiction currently includes pre-approval of privacy policies as a condition, and it is extremely doubtful that any Asia-Pacific jurisdiction would introduce such a requirement.

For businesses in the region, a more attractive proposition will be transferring data to 'adequate' countries or using contracts and other accountability mechanisms to meet the conditions in local legislation. Over time the number of jurisdictions assessed as adequate by the EU and/or other Asia-Pacific jurisdictions should increase. Standard contract terms are already in wide use and there may be further guidance on this from regulators in the future.[51]

Despite these concerns, work on the APEC Privacy Framework continues and some commentators expect Cross Border Privacy Rules to be in use (and presumably 'recognised across APEC') in the near future:

> The Pathfinder Projects should be completed in early 2009. It can be expected that a number of companies will begin to use APEC cross-border privacy rules in the latter part of 2009.[52]

Perhaps this will be true in the Americas or elsewhere in APEC (this Article has not analysed developments in Russia and the Americas). In the Asia-Pacific region it is extremely unlikely that CBPRs will ever become a significant part of the privacy landscape, and there is little chance of their recognition in the region in 2009.

8. Advice and Recommendations

This article has examined current privacy developments in the Asia-Pacific region and provided some analysis of the benefits and risks of pursuing either the EU or US/APEC approach to privacy.

There is a clear and strong trend in the region to protect privacy through comprehensive legislation that is closely aligned with the EU approach. Legislation that is aligned with the EU approach tends to easily meet the self-described 'moderate' Principles contained in the APEC Privacy Framework.[53]

---

[51] *ALRC Report 108*, recommendation 31-7; refer to footnote 20.

[52] Abrams M, *How does 'privacy' translate abroad?*; refer to footnote 49.

The US/APEC approach, however, is much more than just the Principles. The real focus is on the APEC Cross-Border Privacy Rules.

It is difficult to see any benefit for either government or businesses in the Asia-Pacific to adopt Cross-Border Privacy Rules. There may be important questions to answer about the amount of time and energy that has already been expended on the development of the APEC CBPRs in comparison to other important privacy issues.

For governments in the region, the comparison is fairly simple. The US/APEC approach has a significant focus on the registration of business policies with regulators. This is a step that can be avoided, as shown by the success of Canada's privacy legislation in both achieving EU adequacy and delivering user-friendly privacy protection. Great care needs to be taken in the Asia-Pacific to ensure that the region does not import the worst aspects of the EU approach (registration requirements) through adherence to the US/APEC proposals for a CBPR regime.

From a regulator / government perspective CBPRs also represent a significant cultural change. The Asia-Pacific region currently has a low-cost complaints based privacy culture. Local regulators have no skills or experience relevant to the pre-approval of global business policies. No resources are currently allocated to this function, and the budgets of existing privacy regulators in the region are limited. There will also be significant questions about the liability of a regulator who pre-approves (or rejects) the business policy of an organisation in circumstances where the approval carries APEC-wide recognition.

For business, CBPRs look like an expensive investment, with no guarantee of wide adoption:

> It remains unclear to most commentators, and to civil society stakeholders, what real benefits the APEC CBPR approach offer businesses, except perhaps a few information intensive multi-nationals who wish to outsource data processing to a range of different countries and can afford to devote substantial resources to writing the documents and getting them assessed. The vast majority of businesses, including most small and medium sized enterprises in all countries, would almost certainly prefer clear legal obligations, enforced only in the event of a breach, and in the knowledge that outsourcing to some destinations was 'off-limits'.[54]

There is a real risk that unnecessary and expensive registration requirements will be imported into the Asia-Pacific regime for the first time. This should be resisted.

Perhaps a lesson here is that the motivation for the APEC Privacy Framework has had an unnecessary influence on any potential outcomes for the Asia-Pacific. Rather than developing solutions that helped to integrate the APEC Privacy Framework with the EU Directive and the existing privacy regimes in the region, the US/APEC approach has ignored vital elements of the EU approach.

Indeed, in the entire 6,323 words of the APEC Privacy Framework there is not a single mention of Europe, the EU Directive, or any European laws, despite their dominant position in the global privacy landscape.

---

[53] Privacy International, *PI presentation to Asia-Pacific Meeting (Lima, Peru)*, 23 February 2008, <http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-561713>.

[54] Waters N, *The APEC Asia-Pacific Privacy Initiative – a new route to effective data protection or a Trojan horse for self-regulation?*; refer to footnote 19.

Even some US commentators are now recognising the APEC Privacy Framework as a lost opportunity to consider how the EU approach and the APEC approach could work together or be integrated in a way that benefited business:

> At present, it is unclear if and how the initiatives in the EU and APEC can come together to achieve a global solution to international data transfer issues. One thing is clear, however: regional solutions alone will not be sufficient to resolve this issue… While the initiatives in the EU and in APEC are laudable, regional solutions do not address the need for free information flow while protecting privacy.[55]

In practice, the US/APEC approach has found little traction in the region, and work continues apace on the drafting and implementation of EU style legislation across the region:

> 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… that they are well advanced with the introduction of an information privacy law… [56]

It may be useful to conclude this article with some predictions about the future privacy landscape in the Asia-Pacific region.

In 2006, commentator Graham Greenleaf made the following prediction:

> The attraction to countries in the Asia-Pacific of a blanket finding of 'adequate' for their laws will persist. The ideological motivation behind some of the proponents of the APEC process, particularly those in Australia and the USA, to form an 'APEC bloc' that either explicitly rejected or ignored any European privacy standards… has not yet succeeded in fashioning APEC into any such thing. It will probably fail to do so, and the attraction of 'EU adequacy' will persist over time and will influence many aspects of future Asia-Pacific privacy laws.[57]

Although that prediction was made from a privacy advocacy perspective, the issues raised should also be of concern to businesses in the region.

From a broader perspective, this Article makes the following predictions:

— **1.** The APEC Privacy Framework will not be implemented as stand-alone legislation in Asia-Pacific countries. Where it is considered it will have minimal influence on the content of legislation, with perhaps only *Principle 9 – Accountability* having any significant uptake.

— **2.** The APEC Cross-Border Privacy Rules will not be 'recognised across APEC' – certainly not among the Asia-Pacific members and certainly not in 2009. If CBPRs are implemented at all their recognition will be limited to a minority of jurisdictions and their impact will be minimal.

— **3.** Some of the APEC Privacy Pathfinder Projects on administrative matters (such as a contacts directory) may be implemented and will prove useful.

---

[55] Wugmeister M, Retzer K, Rich C, *Global Solution For Cross-Border Data Transfers: Making The Case For Corporate Privacy Rules*, page 20; refer to footnote 11.

[56] Waters N and Lawson P, *Report from representatives of civil society on meetings in Lima, Peru*, February 2008 <http://www.bakercyberlawcentre.org/ipp/publications/Civil_Society_Report_APEC_Lima08.pdf>.

[57] Greenleaf G, *Asia-Pacific Developments in Information Privacy Law and its Interpretation*, University of New South Wales Faculty of Law Research Series, Paper 5, 2006, <http://law.bepress.com/cgi/viewcontent.cgi?article=1007&context=unswwps>.

— **4.** The focus of cross-border privacy protection in the Asia-Pacific region will remain on the use of legislative conditions for data transfers, complemented by the provision of useful and practical alternatives for business compliance, such as standard contract terms. Regulation will remain 'complaints based' in the majority of jurisdictions.

— **5.** The overall standard of privacy protection in the region will improve, and over time national laws will be harmonised through the work of local regional organisations and law reform bodies. Over time, a growing number of jurisdictions will be recognised as 'adequate' by the EU and by each other.

9. Appendix 1 – National Laws

9.1. Australia

The *Privacy Act 1988* (Cth) was amended in 2001[58] to include ten National Privacy Principles (NPPs) that apply to parts of the private sector (those that earn more than $3 million annually). The *Privacy Act* also includes a complaints, audit and enforcement regime.

The privacy regulator is the Office of the Privacy Commissioner.[59] They are a relatively 'light touch' regulator with a history of conciliating disputes.

NPP 9 currently prohibits transfers of personal information by an organisation to someone in a foreign country unless one of six conditions (a) – (f) is satisfied. If one of the conditions is satisfied, then the Australian organisation transferring the data may not be liable under the Act for any privacy breaches which may occur subsequently.

The most relevant conditions are (a) and (f):

- **Condition (a)** allows transfers to recipients in foreign countries who are subject to substantially similar provisions as the NPPs. This requirement is merely that the organisation holds a 'reasonable belief' that the overseas arrangement 'effectively upholds' privacy principles substantially similar to those in the Australian Act. There is no objective or expert determination by a government or Privacy Commissioner of which overseas countries have substantially similar laws or obligations.

- **Condition (f)** allows the transfer if the organisation has taken reasonable steps to ensure that the information transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

In August 2008 the Australian Law Reform Commission (ALRC) *Report 108 – For Your Information: Australian Privacy Law and Practice Report* was released. It contained detailed recommendations on Cross-border Data flows.

> The ALRC's recommended approach to accountability under the 'Cross-border Data Flows' principle draws on the APEC concept of accountability, but takes it further…The ALRC's recommended approach provides for an agency or organisation to remain responsible under Australian privacy law in respect of the actions taken by a recipient of personal information outside Australia. Placing responsibility on the agency or organisation transferring the personal information ensures that an individual has the ability to seek redress from someone in Australia if the recipient breaches the individual's privacy.[60]

However, in introducing a broad accountability requirement as the default protection for cross-border transfers, the ALRC did not recommend the repeal of the other alternative conditions (e.g. consent, substantially similar protection and contractual protection). These will remain in place. The ALRC did recommend some minor improvements:

---

[58] *Privacy Amendment (Private Sector) Act 2000* (Cth), <http://www.comlaw.gov.au/ComLaw/Legislation/Act1.nsf/asmade/bytitle/3E8F716C0779E822CA256F72000B40F8>.

[59] <http://www.privacy.gov.au>

[60] *ALRC Report 108*, chapter 31; refer to footnote 20.

> It should be an exception to the default position of accountability if the agency or organisation transferring the personal information outside Australia reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to the model UPPs.
>
> The ALRC does not recommend that any change be made to the 'reasonable belief' test. It does recommend, however, that the Australian Government should develop and publish a list of laws and binding schemes that effectively uphold principles for fair handling of personal information that are substantially similar to the model UPPs.[61]

These reforms are expected to be implemented in Australia in 2010.

Australia is a member of APEC and chaired the APEC Data Privacy Sub-Group during key stages of the development of the Pathfinder Projects. Australia is also a member of the Pacific Islands Forum.

9.2. Brunei

Brunei is one of the smallest countries in the region. It has no current legislation on privacy.

Brunei is a Member of APEC and attended an APEC privacy capacity building workshop in 2005 – *Technical Assistance Seminar: Domestic Implementation of the APEC Privacy Framework*.[62] There has been no further participation in APEC.

Brunei is also an ASEAN Member Country and shares a commitment to harmonised data protection laws in ASEAN by 2015.

There are no other relevant developments or plans in Brunei.

9.3. Cambodia

Cambodia has no current legislation on privacy.

Cambodia is not a member of APEC.

Cambodia is an ASEAN Member Country and shares a commitment to harmonised data protection laws in ASEAN by 2015.

There are no other relevant developments or plans in Cambodia.

---

[61] *ALRC Report 108*, paragraphs 31.136–31.137; refer to footnote 20.

[62] Greenleaf G, *A Tentative Start For Implementation Of APEC's Privacy Framework*, 2005, <http://www.austlii.edu.au/au/journals/PLPR/2005/16.html>.

9.4. China

In China, rapid economic growth and the benefits of globalisation have come hand in hand with a number of privacy issues which citizens are facing in daily life. National concerns have stemmed from the growing number of reports alleging the selling of personal information to call centres and service providers, as well as the abuse of other readily available personal information (such as the details given in application forms).[63] This exploitation of personal information has resulted in unwelcome phone calls, identity theft and a growing push for legislated privacy law.[64]

Some limited 'freedom and privacy of correspondence' exists in the Chinese constitution as a fundamental right,[65] but there is no consolidated national data protection legislation at this stage. Some minor specific privacy provisions appear in Chinese regulation of spam and ID cards.[66]

In 2003 the State Council's Informatization Office (SCITO) began drafting information laws.[67] While the submission of the initial draft in 2005 did not lead to implementation, it operated as a foundation for the drafting of Data Protection Laws in 2007.[68] The law is now being developed under the new Ministry of Industry and Information Technology. The draft legislation is currently the subject of further stakeholder consultation and expert advice.[69]

The development of Data Protection Laws is being driven and supported by the EU-China Information Society Project (EUCISP), who held a workshop on 14 June 2007. The Workshop unveiled a report on *Personal Data Protection in Europe and China: What Lessons to be Learned*.[70] The report, through an analysis of the successes and failings of EU Data Protection measures, proposes twenty recommendations for Chinese policy-makers.

---

[63] Xu M, Chinese netizens want law to protect their personal information, 28 November 2007, <http://blawg.lehmanlaw.com/english/archives/2007/11/28/418.html>.

[64] Xinhua News Agency, *Lawmaker Urges Legislation to Curb Rampant Privacy Infringement*, 6 March 2005, <http://www.china.org.cn/english/2005lh/121920.htm>.

[65] Article 40, *Constitution of the People's Republic of China 1982* (China), <http://english.people.com.cn/constitution/constitution.html>.

[66] Kim Y, *Data Security, Privacy in Asia – Countries Need to Cooperate for Better Legal Context*, 2007, <http://theseoultimes.com/ST/?url=/ST/db/read.php?idx=6879>.

[67] People's Daily Online, *China to legislate for protection of personal information*, 25 January 2005, <http://english.peopledaily.com.cn/200501/25/eng20050125_171801.html>.

[68] China Economic Net, *Law on personal info 'next year'*, 6 August 2007, <http://en.ce.cn/National/Politics/200708/06/t20070806_12435867.shtml>.

[69] China View, *New law expected to protect privacy*, 6 August 2007, <http://news.xinhuanet.com/english/2007-08/06/content_6480490.htm>; see also Zhe Z, *Law on personal info 'next year'*, China Daily, 6 August 2007, <http://chinadaily.com.cn/china/2007-08/06/content_5448419.htm>.

[70] EU-China Information Society Project, *Research Final Workshop: 'Personal Data Protection'*, 20 June 2007, <http://www.eu-china-infso.org/Regulation/regulation094158@2007-06-20.html>.

A key consideration in China is whether its remarkable growth as an economic powerhouse can be sustained without the implementation of modern laws:

> The relevance for China is obvious: only if China establishes a reliable and robust personal data protection regime will it ensure that trade relationships with the EU (but also with most other countries of the Western hemisphere) can continue to develop. Personal data can easily be called the most valuable resource of the early 21st century. Any responsible country will seek to treat these data with the care they deserve. If for no other reason, the Chinese government's work on a personal data protection law and policy deserves all possible support.[71]

To date, china's draft legislation has been closely aligned with the EU Data Protection Directive.[72] Although their expert advisers have suggested that they should not import some of the more bureaucratic provisions in the Directive:

> Recommendation: Do not require registration – The requirement to register personal data processing centrally has proven administratively burdensome and to add little value and should not be adopted.[73]

China is likely to explicitly seek an EU assessment regarding the adequacy of their laws:

> The concept of 'adequacy' that the EU Data Protection Directive defines is important to the Chinese, and European regulators will expect significant clarification of the enforcement mechanism as a crucial part of any adequacy assessment for China.[74]

Early drafts of the Chinese legislation also include conditions for the cross-border transfer of data:

> Grounds for restrictions are that state security or other significant state interests may be involved, where China has duties under international law, where other laws restrict transfers, and where the recipient country or area does not give 'sufficient' legal protection. The agency in charge of information resources of the State Council will determine which countries or areas come within this last category.[75]

Like many countries in the region, China receives input, funding and advice from both European[76] and US experts[77] on its privacy legislation. China is a member of both ASEM and APEC. While it would appear that China's draft legislation is closely aligned with the EU approach at this stage, the region awaits the final outcome with interest.

---

[71] Sutton G, Xinbao Z, Hart T, *Personal Data Protection in Europe and China: What lessons to be Learned?*, EU-China Information Society Project, November 2007, <http://www.ucl.ac.uk/constitution-unit/foidp/downloads/Personal_Data_Protection_Public_CB_final_29_10_2007.pdf>; see also Robertson S, *Privacy and outsourcing to China*, January 2008, <http://www.galexia.com/public/research/articles/research_articles-art49.html>.

[72] Greenleaf G, *China proposes Personal Information Protection Act*, Privacy Laws & Business International Newsletter, February 2008, issue 91.

[73] Sutton G, Xinbao Z, Hart T, *Personal Data Protection in Europe and China: What lessons to be Learned?*; refer to footnote 71.

[74] Treacy B and Abrams M, *A privacy law for China?*, Complinet, 29 May 2008, <http://www.hunton.com/files/tbl_s47Details/FileUpload265/2269/privacy_law_for_China.pdf>.

[75] Greenleaf G, *China proposes Personal Information Protection Act*; refer to footnote 72.

[76] Sutton G, *Legislating for data protection in China*, Dataprotectionreview.eu, 4 October 2007, <http://www.madrid.org/cs/Satellite?c=CM_Revista_FP&cid=1142393109240&esArticulo=true&idRevistaElegida=1142392620578&language=en&pagename=RevistaDatosPersonalesIngles%2FPage%2FRDPI_home_RDP>.

[77] The Centre for Information Policy Leadership, *China Privacy Governance*, Hunton & Williams LLP, June 2007, <http://www.hunton.com/files/tbl_s47Details/FileUpload265/1944/China_Privacy_Two-Pager.pdf>.

9.5. Hong Kong

Hong Kong has established comprehensive privacy legislation for the private sector in the *Personal Data (Privacy) Ordinance 1995*.[78] The legislation is broadly aligned with the EU Data Protection Directive, although the Data Protection Principles are significantly shorter and simpler. Hong Kong has not introduced any registration requirements for businesses.

Section 33 of the *Hong Kong Personal Data (Privacy) Ordinance 1995,* is not currently in force. Once implemented, section 33(2) will forbid onward transfer of personal data outside of Hong Kong, unless, one of the stipulated situations apply. The conditions are similar to those in the Australian Act (NPP 9) with one significant difference. The Hong Kong provision allows the Privacy Commissioner[79] to designate a jurisdiction with substantially similar privacy laws to Hong Kong's Ordinance.

As Section 33 is not yet in force and there are not yet any designated jurisdictions, much reliance can be placed on condition (b), that the organisation reasonably believes that the privacy laws of the recipient's country are substantially similar to Hong Kong's Ordinance.

Hong Kong is a member of APEC.

9.6. Indonesia

Indonesia is a member of APEC, but is not an active participant in the APEC Privacy Pathfinder Projects. Indonesia is also a member of ASEAN and has committed to the development of harmonised data protection legislation by 2015.

There is currently no comprehensive privacy legislation in Indonesia, although their umbrella e-commerce law does contain a privacy commitment – this requires subsequent detailed regulations. Privacy may not be a high priority area in Indonesia compared with current issues such as digital copyright and online content regulation.

The *Law on Information and Electronic Transactions*[80] is an ambitious piece of umbrella legislation covering e-government, electronic contracting, privacy, cybercrime, digital copyright and other cyberlaw issues in a single omnibus Law. The legislation contains a single, brief provision on privacy:

> Article 26
>
> (1) The utilization of any information by means of electronic media relating to data about private right of anyone shall be carried out with the approval of the person concerned unless otherwise stipulated by the statutory regulation.
>
> (2) Any person whose rights are violated in the manner detailed in paragraph (1) is entitled to compensation for any loss as explained within this legislation.

The provision necessitates consent for any electronic use of personal data, by the person whom the data relates to, except in cases where statutory legislation negates this requirement.

---

[78] *Personal Data (Privacy) Ordinance 1995* (Hong Kong), <http://www.pcpd.org.hk/english/ordinance/ordfull.html>.

[79] <http://www.pcpd.org.hk/engindex.html>

[80] Galexia, *Indonesian Parliament passes e-commerce law*, March 2008, <http://www.galexia.com/public/about/news/about_news-id127.html>.

The privacy measures afforded by Article 26 of the *Law on Information and Electronic Transactions* are a small step on the road to a more secure e-commerce environment. The provision echoes elements of the various international instruments. While a fuller implementation of privacy legislation in the future may be a goal of the Indonesian legislature, Article 26 provides a foundation for the protection of individuals' privacy rights.

Indonesia is an ASEAN Member Country and shares a commitment to harmonised data protection laws in ASEAN by 2015.

9.7. Japan

The *Act on the Protection of Personal Information 2003*[81] is a very comprehensive piece of privacy legislation with detailed rules on almost every aspect of personal information management. The *Act* is supplemented by Guidelines issued by relevant government agencies – there are more than 35 in place.[82] There is no single privacy regulator in Japan. Instead, other government regulators are responsible for policing privacy compliance in particular industries.[83]

Article 23.1 of the *Act on the Protection of Personal Information 2003* sets out a general prohibition on the transfer of personal data to any third party without the prior consent of the data subject.

Article 23.4 of the Act allows the sharing of information in certain circumstances. Article 23.4(1) covers the situation where personal data is entrusted to another person or entity such as a data-processing company or an outsourced company handling payroll. To the extent necessary to achieve the purpose of use of that personal data, the entity may transfer the data without obtaining the consent of the data subject.

However, under Article 22, organisations are responsible for the supervision of such delegates for proper handling of personal data. For example, the *Guideline for Personal Information Protection in the Financial Services Sector* requires that the entity must enter into an agreement setting out the responsibilities of such delegates to protect the personal data.

In addition to the legislation, many Japanese companies participate in a voluntary privacy trustmark scheme that indicates compliance with a local standard: JIS Q 15001.[84] However, the trustmark appears to be only used by domestic Japanese firms: 'Companies eligible to receive certification for PrivacyMark are private enterprises based in Japan'.[85]

Japan is a member of APEC.

---

[81] *Act on the Protection of Personal Information 2003* (Japan), <http://www5.cao.go.jp/seikatsu/kojin/foreign/act.pdf>.

[82] Ponazecki J, Levison D, *World Data Protection Report – Japan: Personal information privacy update*, BNA International, December 2007, <http://www.mofo.com/docs/pdf/WDPR1207_Privacy.pdf>.

[83] Miyashita H, *A Japanese Culture of Privacy*, Technical Assistance Seminar on International Implementation of the APEC Privacy Framework, 18 February 2008, <http://aimp.apec.org/Documents/2008/ECSG/SEM1/08_ecsg_sem1_008.pdf>.

[84] Japan Information Processing Development Corporation, *PrivacyMark System*, 1 August 2008, <http://privacymark.org/news/2008/0801/ThePrivacyMarkSystem_Aug_1_2008.pdf>.

[85] <http://privacymark.org/application/new/qualification.html>

9.8. Korea

South Korea's privacy law is contained in the *Act on the Protection of Personal Information Maintained by Public Agencies 1999*[86] for Government and the *Act on Promotion of Information and Communication Network Utilization and Information Protection 2001*[87] for the private sector. This second Act only applies to the information and telecommunications industries that are providers of information and communications services such as common carriers, Internet service providers and other intermediaries, such as content providers. The Act also covers specific offline service providers such as travel agencies, airlines, hotels, and educational institutes.

However, there is a significant push for reform of privacy law in Korea. During 2007 three bills were awaiting debate at Korea's Government Administration and Home Affairs Committee. The Ministry of Information and Communication has also drafted a revised version of the current Act. The revised draft takes into account the unique characteristics of the IT sector as well as the rising demand for stronger personal information protection. The draft also improves upon the existing law and addresses the issues that were raised during enforcement of the law.[88]

The current privacy regulator is the Ministry of Information and Communication as they provide guidance for any services provided via websites or information technology. The key regulator is the Korea Information Security Agency (KISA), although complaints handling is complemented by the work of the Personal Information Dispute Mediation Committee (PICO).[89]

Article 54 is relevant to the transfer of personal data to other jurisdictions. It prevents the entity from entering into an international contract that might violate the information protection provisions. In effect, this is requiring that any transborder data flow to another jurisdiction must only occur where there is the same or higher protection for data as that set out under the Act.

In July 2008, the Korean Cabinet agreed to expand and enhance Korea's data protection laws:

> The Korean government… would take measures for heightened privacy protection to address public concerns over the illegal use of personal information. The government will expand its budget for the protection of personal data and enforce tougher privacy rules on companies, under the plan announced at the Cabinet meeting involving the Ministry of Public Administration and Security, the Ministry of Knowledge Economy, the Korea Communications Commission and the National Intelligence Service and Prime Minister Han Seung-soo… The government will draw up a data protection bill during the second half of this year, including prohibiting firms from obtaining customer data except in certain cases.[90]

Korea is a member of APEC.

---

[86] *Act on the Protection of Personal Information Maintained by Public Agencies 1999* (Korea), <http://www.kca.go.kr/web/img/eng/1_1 ACT ON THE PROTECTION OF PERSONAL INFORMATION MAINTAINGED BY PUBLIC AGENCIES.doc>.

[87] *Act on Promotion of Information and Communications Network Utilization and Information Protection 2001* (Korea) <http://www.ecommerce.or.kr/activities/policy_view.asp?bNo=336&Page=1>.

[88] National Internet Development Agency of Korea, *Korea Internet White Paper 2006*, 21 July 2006, page 78, <http://www.mic.go.kr/eng/secureDN.tdf?seq=10&idx=1&board_id=E_04_03>.

[89] Greenleaf G, *A Tentative Start For Implementation Of APEC's Privacy Framework*; refer to footnote 62.

[90] Sojung Y, *Gov't to enhance privacy protection*, Korea.net, 23 July 2007, <http://www.korea.net/News/News/NewsView.asp?serial_no=20080723011>.

9.9. Laos

Laos is a small developing country and remains on the UN list of least developed countries. Laos has no current legislation on privacy.

Laos is not a member of APEC.

Laos is an ASEAN Member Country and shares a commitment to harmonised data protection laws in ASEAN by 2015.

There are no other relevant developments or plans in Laos.

9.10. Macau

Macau is now a Special Administrative Region of China, however it maintains its own suite of commercial laws.

Macau has comprehensive privacy legislation in the form of the Personal Data Protection Act (2005).[91] The regulator is the Office for Personal Data Protection.[92]

Article 19 of the Act contains principles relevant to the cross-border transfer of personal data.

> Article 19-1 – The transfer of personal data to a destination outside the MSAR may only take place subject to compliance with this Act and provided the legal system in the destination to which they are transferred ensures an adequate level of protection.

Macau is not a member of APEC or any other regional organisation. The Macau Office for Personal Data Protection has been participating in meetings of the Asia Pacific Privacy Authorities (APPA).

9.11. Malaysia

Increasing understanding of the risks associated with personal data in Malaysia has seen a push for a *Data Protection Act* and after a long and complex history,[93] Malaysia's *Personal Data Protection Bill* is now in the final stages of drafting.[94] The Bill is expected to be subject to a further round of stakeholder consultation in late 2008.[95] Some stakeholders are encouraging Malaysia to enact legislation that meets the standards of the EU Directive.[96]

---

[91] *Personal Data Protection Act (Act 8/2005)* (Macau) <http://www.gpdp.gov.mo/cht/forms/lei-8-2005_en.pdf>.

[92] <http://www.gpdp.gov.mo/en/>

[93] Jawahitha S, Ishak M and Mazahir M, *E-Data Privacy and the Personal Data Protection Bill of Malaysia*, Centre for Cyberlaw, Faculty of Management, 2007, <http://www.ansijournals.com/jas/2007/732-742.pdf>.

[94] The Star, *Act to keep personal data private*, 6 November 2007, <http://thestar.com.my/news/story.asp?file=/2007/11/6/parliament/19387238>.

[95] The New Straits Times, *After 10 years in limbo, your privacy remains at stake*, 13 January 2008, <http://www.nst.com.my/Current_News/NST/Sunday/National/2131002/Article/index_html>.

[96] Human Rights Committee, *HRC Responds: Consult stakeholders on the proposed Data Protection Bill*, The Malaysian Bar, 16 July 2008, <http://www.malaysianbar.org.my/human_rights/hrc_responds_consult_stakeholders_on_the_proposed_data_.html>.

The Bill provides ambitious, comprehensive privacy protection:

> The personal data protection law is envisaged to be a world class leading edge cyberlaw that provides for higher level of personal data protection… and to promote Malaysia as a preferred trading partner that provides international standards of personal data protection.[97]

There are also proposals in Malaysia to establish both a Privacy Commissioner and a Personal Data Protection Tribunal (to hear appeals from decisions of the Commissioner). Malaysia has looked at all options, including the EU and APEC approaches in drafting their legislation.[98]

Malaysia is an ASEAN Member Country and shares a commitment to harmonised data protection laws in ASEAN by 2015.

9.12. Myanmar

Myanmar is a relatively isolated country with a large population. It has surprisingly advanced laws in many areas of e-commerce but there is no current legislation on privacy.

Myanmar is not a member of APEC.

Myanmar is an ASEAN Member Country and shares a commitment to harmonised data protection laws in ASEAN by 2015.

There are no other relevant developments or plans in Myanmar.

9.13. New Zealand

New Zealand has comprehensive privacy legislation – the *Privacy Act* 1993 – regulated by an independent Privacy Commissioner. There is an expectation that New Zealand may be assessed as adequate by the EU once trans-border data provisions in the legislation are strengthened.[99]

New Zealand itself is committed to amending the legislation and seeking an EU Adequacy assessment by 2011:

> The Privacy Act [will be] amended to harmonise with EU requirements for transborder transfers of personal data, in order to strengthen New Zealand's case for 'white list' status under the EU Directive.[100]

---

[97] Minister of Energy, Communications & Multimedia (Malaysia), *Presentation of Personal Data Protection Bill to Participants of the Asian Personal Data Privacy Forum (Hong Kong)*, 27 March 2001, <www.pcpd.org.hk/misc/malaysia/Malaysia.ppt>.

[98] Bernama, *Ministry Finalising Draft of Personal Data Protection Bill*, 5 November 2007, <http://www.ktak.gov.my/template03.asp?tt=news&newsID=375>.

[99] Office of the Privacy Commissioner (NZ), I*nternational Transfers of Personal Data: Candidate for Adequacy – The New Zealand Case*, 8 July 2001, <http://www.privacy.org.nz/international-transfers-of-personal-data-candidate-for-adequacy-the-new-zealand-case/>.

[100] Office of the Privacy Commission (NZ), *Statement of Intent 2008/09*, 2008, page 16, <http://www.privacy.org.nz/assets/Files/SOI-2008-09.pdf>.

Principle 10 of the Act currently extends the application of the information principles to information held overseas:

> 10 Application of principles to information held overseas
>
> (1) For the purposes of principle 5 and principles 8 to 11, information held by an agency includes information that is held outside New Zealand by that agency, where that information has been transferred out of New Zealand by that agency or any other agency.

The steps needed to ensure adequacy for New Zealand have been described as 'minor'.[101]

New Zealand is a member of APEC and has been an active participant in several APEC Privacy Pathfinder Projects. New Zealand is also a member of the Pacific Islands Forum.

9.14. Pacific Islands

The Pacific Islands Forum is a regional organisation comprising Australia, the Cook Islands, Micronesia, Fiji, Kiribati, the Marshall Islands, Nauru, New Zealand, Niue, Palau, Papua New Guinea, Samoa, the Solomon Islands, Tonga, Tuvalu, and Vanuatu. Associate members are New Caledonia and French Polynesia. Observers are Tokelau and Timor-Leste (East Timor).

There are no comprehensive privacy laws in any of the smaller jurisdictions at this stage (excluding Australia and New Zealand), but they have a cyberlaw harmonisation project that may incorporate privacy law in the future.[102]

The Wellington Declaration[103] (made by the Pacific Island Forum Information and Communications Technologies Ministerial Meeting 30 March 2006, Wellington, New Zealand) established some priority areas of concern including identifying assistance for capacity building for regulatory infrastructure. A *Workshop on Principles of Cyber Legislation for Pacific Island Countries* in 2007 included data protection in the list of ICT laws requiring harmonisation.

The current priority in the region is the development of anti-spam legislation – with new legislation in place or drafted for Cook Islands, Niue, Samoa, Tonga and Vanuatu.[104]

It is Important not to underestimate the privacy protection that exists in some of the small Pacific nations, or to assume that protections are non existent, as some minor privacy law provisions exist in the constitutions and/or common law of individual member countries, and there is some local case law on the invasion of privacy.[105]

---

[101] Slane H, *Human Rights in Foreign Policy*, Office of the Privacy Commissioner (NZ), 6 September 2000, <http://www.privacy.org.nz/human-rights-in-foreign-policy/>.

[102] Pacific Islands Forum Secretariat, Pacific Regional Digital Strategy, November 2006, <http://www.forumsec.org.fj/UserFiles/File/Regional_Digital_Strategy.pdf>.

[103] Forum Information and Communications Technologies Ministerial Meeting, *Wellington Declaration,* 30 March 2006, <http://www.forumsec.org/UserFiles/File/Wellington_Declaration.pdf?phpMyAdmin=a2498005399765db990bdeaef994e9d1>.

[104] Galexia, *DBCDE – Strengthening Span Legislation, Enforcement and Cooperation Regimes in the Pacific project*, October 2007, <http://www.galexia.com/public/projects/projects-DBCDE.html#Heading41>.

[105] See for example *Mauricio v Phoenix of Micronesia Inc* [1998] FMSC 23; 8 FSM Intrm. 411 (Pon. 1998), 3 August 1998, <http://www.paclii.org/cgi-bin/disp.pl/fm/cases/FMSC/1998/23.html> and *Nethon v Mobil Oil Micronesia, Inc.* [1994] FMSC 22; 6 FSM Intrm. 451 (Chk. 1994), 11 July 1994, <http://www.paclii.org/cgi-bin/disp.pl/fm/cases/FMSC/1994/22.html>.

Vanuatu is the only country with any specific privacy legislation. The Vanuatu Electronic Transactions Act 2000[106] contains the following section on data protection:

> 25 (1) The Minister may make orders prescribing standards for the processing of personal data, whether or not the personal data originates inside Vanuatu.
>
> (2) The regulations may provide for the following:
>
> (a) the voluntary registration and de-registration to the standards by data controllers and data processors;
>
> (b) the establishment of a register that is available for public inspection showing particulars of data controllers and data processors who have registered or de-registered to the standards and the dates thereof and the countries in respect of which the registration applies;
>
> (c) the application of the standards to those countries specified in the regulations;
>
> (d) different standards to be applied in respect of personal data originating from different countries.

At the time of writing no orders have been made under this Section.

9.15. Philippines

The Philippines is in the process of developing comprehensive privacy legislation. Several Bills are currently before their Parliament and these are expected to be combined into a final draft Bill in the near future. The legislation aims to:

> Establish fair practices in the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, dissemination by any means, merging, linking, blocking, erasure or destruction of personal data of natural persons and to penalise the unauthorised processing and disclosure thereof.[107]

The early drafts of the legislation were 'influenced by the structure and the language of the EU Directive and the UK's Data Protection Act of 1998'.[108] However, efforts are currently being made to ensure that some of the more bureaucratic registration requirements in the EU Directive are not imported into the Philippines legislation.

The Philippines is a member of APEC and has been attending some APEC Privacy Framework meetings.

The Philippines is an ASEAN Member Country and shares a commitment to harmonised data protection laws in ASEAN by 2015.

---

[106] *Electronic Transactions Act (No. 24 of 2000)* (Vanuatu) <http://www.paclii.org/vu/legis/num_act/eta2000256/>.

[107] Stakeholders are currently consulting on the version of the Bill located at: <http://www.senate.gov.ph/lisdata/547548551.pdf>.

[108] See Parlade C, *Privacy and Data Protection in the Philippines*, Privacy Laws and Business International 2008 (forthcoming).

9.16. Singapore

Singapore is yet to enact data protection legislation, although a voluntary, industry-based self regulatory model code exists. The *Model Data Protection Code*[109] was developed by the InfoComm Development Authority[110] and is based on OECD data protection guidelines.[111] The Model Code is designed to be adopted by businesses in their own data protection policies.

In the absence of specific legislation, the *Model Data Protection Code for the Private Sector* represents best privacy practice in Singapore. It is unlikely that Singapore would be assessed as adequate by the EU, although this issue is the subject of some interest to Singapore businesses.[112]

The Model Code applies to any private sector organisation that collects and installs personal data in electronic form, online or offline, using the Internet or any other electronic media.

> 1.4 The Model Code applies to any personal data which are processed or controlled by the organisation, regardless of whether the data are transferred out of Singapore. The Model Code applies in favour of all persons, whether resident in Singapore or not, whose data are or have been processed by the organisation.

It is important to note that the Model Code was always intended to be an interim measure on a longer path towards comprehensive legislation:

> As an interim measure, voluntary data protection guidelines for the private sector (such as the Model Code) should be given official recognition and adherence invited on a voluntary basis. The exercise will have an educative and harmonising function and should facilitate the introduction of legislation, should Parliament decide in the future to legislate.[113]

In 2006-2007 privacy legislation was the subject of an inter-agency committee study.[114] In 2008, there have been discussions of a new commitment to privacy legislation in Singapore – based on a sectoral approach similar to that used in Japan.

Singapore is a member of APEC. Singapore is not currently participating in any APEC Privacy Pathfinder Projects, but is hosting the meetings of the Data Privacy Sub Group in 2009.

Singapore is an ASEAN Member Country and shares a commitment to harmonised data protection laws in ASEAN by 2015.

Singapore also has a small TrustMark scheme.[115] However, this is a generic e-commerce scheme and does not include specific privacy requirements beyond a requirement to publish a privacy policy on a website.[116]

---

[109] TrustSG, *Model Data Protection Code*, 2003, <http://www.trustsg.com.sg/downloads/Data_Protection_Code_v1.3.pdf>.

[110] <http://www.ida.gov.sg/>

[111] Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980, <http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html>.

[112] Lehdonvirta V, *European Union Data Protection Directive: Adequacy of Data Protection in Singapore*, 2004, Singapore Journal of Legal Studies, pages 511-546, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=953993>.

[113]The National Internet Advisory Committee Legal Subcommittee, *Report On A Model Data Protection Code For the Private Sector*, 2002, <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN012665.pdf>.

[114] Wong M, *Committee reviewing data protection regime in Singapore*, Channel NewsAsia, 16 February 2006, <http://www.infowar-monitor.net/modules.php?op=modload&name=News&file=article&sid=1319&mode=thread&order=0&thold=0>.

[115] <http://www.trustsg.org.sg/index.html>

9.17. Taiwan

Taiwan has complex privacy legislation in place – the *Computer-Processed Personal Data Protection Law 1995* ('the PDP law')[117] regulates the 'computerized processing of personal data'. At present eight categories of non-government organisations ('non-public institution') are governed by it, including those in finance or securities.

The PDP Law requires certain private sector organisations to register their activities with a relevant regulator. Companies who register are bound by the privacy legislation but receive some generous waivers for communications with clients.

There is no central agency responsible for enforcement of the PDP Law. Enforcement is handled by the relevant government authority for the sector concerned.

There have been some high profile privacy breaches in Taiwan in relation to lost/stolen credit card data. Privacy issues are reasonably high on the agenda as a result of these breaches.

Under Article 24 of the PDP Law, the relevant authority for the sector may issue restrictions on particular transborder transfers for any of the four circumstances set out in the Article. Article 24(3) specifies the circumstance similar to the EU's requirement for `adequate protection'. That is, where the receiving country lacks proper laws and / or ordinances to adequately protect personal data and where there are apprehensions of injury to the rights and interests of a concerned party.

Taiwan is currently undertaking substantial reform of privacy legislation.

Taiwan is an APEC member and an active participant in several APEC Privacy Pathfinder Projects.

9.18. Thailand

Thailand has a draft *Privacy Act* that strives to protect an individual's personal information while balancing this with the development of information technology and the promotion of Thailand's ICT policy. The draft data protection law is based on eight principles: consent, notice, purpose specification, use limitation, accuracy, access, security and enforcement.[118]

Businesses have been encouraging Thailand to develop privacy legislation in order to 'seize BPO opportunities'.[119] Thailand is in the final stages of consultation on its draft privacy legislation, under the direction of the Council of State. The general approach taken in the draft legislation is closely aligned with the EU Directive.[120]

Thailand is an APEC member. Thailand is also an ASEAN Member Country and shares a commitment to harmonised data protection laws in ASEAN by 2015.

---

[116] TrustSG, *Self Assessment for Merchants*, 2005, <http://www.trustsg.org.sg/downloads/Self_Assessment_for_Merchants.pdf>.

[117] *Computer-Processed Personal Data Protection Law 1995* (Taiwan), <http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/national_laws/Taiwan-CP-DPLaw.pdf>.

[118] Privacy International, *Privacy and Human Rights 2006 – Kingdom of Thailand*, 18 December 2007, <http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559484>.

[119] Bangkok Post, *We need data privacy act to attract BPO*, 7 February 2007, <http://www.bangkokpost.net/20th_database/07Feb2007_data52.php>.

[120] Raksirivorakul W, *Introducing Thailand's Data Protection Law*, Mayer Brown, 26 June 2008, <http://www.mayerbrown.com/publications/article.asp?id=5053&nid=6>.

9.19. Vietnam

Vietnam does not have comprehensive privacy legislation, but it does have a short privacy section in their e-commerce legislation that could serve as a foundation for more detailed legislation in the future. Article 46 of the *Law on E-Transactions* covers information confidentiality in e-transactions:

> 1. Agencies, organizations and individuals shall have the right to select security measures in accordance with the provisions of the law when conducting e-transactions.
>
> 2. Agencies, organizations and individuals must not use, provide or disclose information on private and personal affairs or information of other agencies, organizations and/or individuals which is accessible by them or under their control in e-transactions without the latter's consents, unless otherwise provided for by law.

In addition, the *Law on Information technology* stipulate that more detailed regulations regarding information protection in the environment such as regulations on collection, process, use, storage and provision of personal information, may be developed in the future (Articles 21 and 22).[121]

Vietnam is also considering the development of a trust-mark scheme, and has made specific references to the APEC Privacy framework in relation to their trust-mark proposal.[122]

Vietnam is an ASEAN Member Country and shares a commitment to harmonised data protection laws in ASEAN by 2015.

[121] Hoang Minh D, *Data Privacy and Data Protection in E-Commerce In Vietnam*, Technical Assistance Seminar on International Implementation of the APEC Privacy Framework (Lima, Peru), 18 February 2008, <http://aimp.apec.org/Documents/2008/ECSG/SEM1/08_ecsg_sem1_013.pdf>.

[122] Vietnam Business Finance, *Data privacy poses obstacle to e-commerce development*, 30 March 2008, <http://www.vnbusinessnews.com/2008/03/data-privacy-poses-obstacle-to-e.html>.

10. Appendix 2 – Asia-Pacific Summary Table

Country	Privacy Legislation	APEC	ASEAN	Pacific Islands Forum
Australia	Comprehensive legislation	√		√
Brunei	None	√	√	
Cambodia	None		√	
China	Draft legislation	√		
Hong Kong	Comprehensive legislation	√		
Indonesia	Single clause in e-commerce law	√	√	
Japan	Comprehensive legislation	√		
Korea	Comprehensive legislation	√		
Laos	None		√	
Macau	Comprehensive legislation			
Malaysia	Draft legislation	√	√	
Myanmar	None		√	
New Zealand	Comprehensive legislation	√		√
Pacific Islands (14 small nations)	Single clause in Vanuatu e-commerce law. No other legislation.			√
Philippines	Draft legislation	√	√	
Singapore	None	√	√	
Taiwan	Comprehensive legislation	√		
Thailand	Draft legislation	√	√	
Vietnam	Single clause in e-commerce law	√	√	