

Chapter 3

Overview of Asian Privacy Law Lessons Learned and Possible Ways Forward

**Malcolm Crompton
Managing Director
Information Integrity Solutions**

Table of Contents

Summary	1
Overview of Trends in Privacy Law in Asia	1
Overview of Australia	3
Overview of Japan	5
Conclusions and Lessons Learned	7
List of Additional References	11
Appendix A	13

Summary

Economies in the APEC region are increasingly adopting privacy laws. Some economies are doing this to address citizen concerns over the safety of online transactions; others want to attract business process off shoring on the basis that personal information of people from other economies will not be compromised. Economies considering having privacy law will benefit from taking into account the wider privacy context. Doing so will help them to avoid some pitfalls which include unnecessarily impeding business activities both domestically and internationally. This is best achieved by looking at the global environment and learning from the experience of other economies. These experiences show that the best outcome for business is privacy law which:

- is principles based;
- is comprehensive across the economy;
- has a consistent approach;
- has minimal exemptions; and
- is enforced in a coordinated way by an independent agency.

To take into account the increasingly global transfer of personal information economies will benefit if their privacy law is consistent with global trends and builds in structures that will allow global cooperation among privacy enforcement bodies where a breach of privacy law involves more than one economy. There is an opportunity to build this into the new law from the beginning, and to take the lead in this area to influence other economies in the region.

Overview of Trends in Privacy Law in Asia

Economies in the Asia-Pacific Economic Cooperation forum are increasingly adopting privacy laws. New Zealand, Australia and Hong Kong were part of the first wave of privacy law in the late 1980s and 90s. In the last year or so the number of economies legislating and implementing privacy law has increased dramatically. Economies in the region considering new or more comprehensive privacy law include China, Chinese Taipei, Indonesia, Malaysia, Mexico (and other economies in South America), Singapore, South Korea, Thailand and Vietnam and more tentatively, India. Japan brought in new comprehensive law in 2003 while Australia and Canada have strengthened their law in the last 5 years. A document that outlines the status of privacy law in a number of Asian and other economies is at Appendix A.

Some economies are considering privacy laws in order to address citizen concerns over the safety of online transactions. Others want to attract business process off shoring and are concerned that they will lose business to other economies unless they can provide assurance that the personal information involved will be protected. At the same time, governments and business do not want to impede business activities in other aspects of their operations or disrupt socially important flows of personal information. Many businesses rely on access to personal information to make contact with new clients, to maintain contact with current clients or to conduct checks on credit or safety checks. For example, if privacy laws are too restrictive, they could have the unintended consequence that companies cannot provide clients or prospective clients with services that they would like to have or lines of credit. Also, laws that require notices about collecting personal information to be dispatched too frequently or in too much detail can create high costs for business with little benefit for individuals who may not be interested in reading detailed legalistic notices.

Governments and business therefore must find a balance that meets both the privacy expectations of their citizens and meets privacy protection requirements of overseas economies seeking offshore services without unduly restricting local business activity. Governments always face strong pressure to develop a balance that is uniquely geared to local interests and conditions. However, the real key to addressing this dilemma is to recognize that these problems have been faced by other economies and there is much to be learned from them. There are a

number of economies that are operating very well with strong privacy laws. The one sure lesson to be learned is that developing a unique solution that does not take into account international trends and experience will be the worst possible outcome for business as well as citizens. Aside from wasted time and effort, it means that the economy will not be ready for the next major stage in privacy law development, which is to ensure that privacy protection operates well within the global economy.

This paper goes on to illustrate some of these points by examining the experience with privacy law of Australia and Japan.

Overview of Australia

The privacy law

Australia first had privacy law in 1988 (The *Privacy Act 1988* (Cwth) (the Privacy Act)). At this time, it only covered personal information held by Australian federal public sector agencies. It established an Office of the Privacy Commissioner and a Privacy Commissioner and includes 11 Information Privacy Principles (IPPs). The 11 principles are based on the Organisation for Economic Cooperation and Development (OECD) privacy principles and govern the collection, use, storage, access to, maintenance and disclosure of an individual's personal information.

In 1990, the Privacy Act was amended to regulate the handling of credit reports and other credit worthiness information about individuals held by credit reporting agencies and credit providers.

In 1998, following extensive consultation, the Privacy Commissioner issued the National Principles for the Fair Handling of Personal Information (the National Principles), compliance with which was voluntary. This was partly in response to a directive on information privacy adopted in October 1995 by the European Parliament and the Council of the European Union (EU) which included a provision that personal data could not be transferred from an EU country to a non-EU country unless there was an adequate level of information privacy.

In late 1998, the Government announced its intention to legislate to support and strengthen privacy protection in the private sector. After widespread consultation the Privacy Amendment (Private Sector) Act 2000 was passed in December 2000 with a commencement date of 21 December 2001. It aimed to establish a single comprehensive national scheme governing the collection, holding, use, correction, disclosure and transfer of personal information by private sector organisations. It did so by means of the National Privacy Principles (NPPs) and provisions allowing organisations to adopt approved privacy codes. The NPPs are also based on the OECD principles, however they are different from the IPPs governing the Australian government public sector, in order to fit the way private sector organizations operate.

The main reasons for having general privacy laws that covered the private sector were:

- the potential for barriers to international trade for business
- the lack of protection afforded to the consumer
- the effects on the take-up of electronic commerce resulting from lack of protection to consumers
- the lack of comprehensive coverage of business
- the possibility that some State and Territory governments within Australia would impose stricter controls which would result in inconsistencies between jurisdictions.

The privacy law applying to the private sector in Australia is intended to be a 'light touch', 'principles based' approach which takes into account the general desirability of the free flow of information and the right of government and business to achieve their objectives in an efficient

way. The principles are explained by non-binding guidelines and information sheets written by the Office of the Privacy Commissioner.

The Privacy Act is enforced by the Office of the Privacy Commissioner which is an independent body set up under the Privacy Act. The Attorney-General appoints the Privacy Commissioner, usually for a 5 year term. The Attorney-General can only dismiss the Privacy Commissioner in very limited circumstances. The Commissioner mostly enforces the law through the Office's complaints process, but also has the power to take action in court to prevent an action taken or proposed by a government agency or private sector organisation. Except for the enforcement of credit reporting provisions the Office does not have the power to audit private sector organisations but can initiate investigations without waiting for a complaint.

The private sector provisions of the Privacy Act have a number of exemptions that limit the extent of their application. Exemptions include for small businesses (unless they are providing health services, services to the government or are buying or selling personal information), employee records, politicians and political parties and the media. The law applies to about 70 percent of Australian business activity.

Impact of law

Most businesses had 12 months in which to prepare before the private sector privacy provisions came into effect. However, guidelines were not available until just before the private sector provisions came into effect. Some businesses wanted very non-prescriptive guidelines to explain how the privacy principles worked. Others wanted much more information about how to comply with the privacy provisions. Small businesses that were not exempted from the private sector provisions needed more help to implement the privacy principles. They had two years to prepare.

The Office of the Privacy Commissioner reviewed the private sector provisions of the Privacy Act in 2004-2005, after the Privacy Act had been in operation for 3 years. There was extensive consultation with business on how well the Privacy Act is working. Overall, business was happy with the private sector provisions and the balance they strike between privacy protection and the need to enable business to operate in an efficient way. Consumer groups were less satisfied with the law.

However, business did raise some concerns about how the private sector privacy provisions are operating. These include concern that there are too many inconsistent privacy laws applying to business and that many of these laws overlap. These laws also establish their own privacy enforcement body separate from the federal Office of the Privacy Commissioner. This happened because in addition to the Privacy Act, some State and Territory Governments passed privacy laws which also apply to business. This is especially so in the health area. A number of businesses also thought that there are too many exemptions in the Privacy Act and that this combined with many and overlapping laws and privacy law enforcement bodies makes compliance complicated and increases costs. A number of businesses also said that the Office of the Privacy Commissioner should have more resources so that it can handle complaints more quickly and so that it can put more effort into educating business and consumers about how the Privacy Act operates. Some businesses were concerned that currently there is not enough incentive for businesses to comply with the Privacy Act because there is a very low risk that those that fail to comply with the Privacy Act will be caught, and even if caught, there are no real penalties. They argued that this disadvantages companies that have put in a lot of effort in to complying with the Privacy Act.

A further issue that emerged from the review is that many companies were obtaining consents for collection, use and disclosure of personal information under the Privacy Act by using long and hard to understand privacy notices. In some cases businesses were seeking consent when they did not need to. In many cases, consumers had no real choice about giving their consent and so were not gaining the protection the privacy principles were intended to provide.

The review of the private sector provisions of the Privacy Act also found that the Act and the privacy principles may not be keeping up with developments in technology and rapid globalization. The Government has now established a further review to look into this issue, as well as other aspects of the Privacy Act. The review is being carried out by the Australian Law Reform Commission.¹ Research has also established that the Office of the Privacy Commissioner has limited ability to cooperate with enforcement authorities in other economies which makes it difficult to protect personal information that is collected, used or disclosed inappropriately outside Australia. Although one of the reasons for having private sector privacy law was to enable Australian businesses to more easily transfer information to economies in the European Union and vice versa, Australia's law has not achieved the necessary 'adequacy' status with the European Union for this to occur. The exemption for small business appears to be one reason for this. For more information about the European Union approach to the international transfer of personal information, see Christopher Kuner's paper: *Overview of European Privacy Law*.

Overview of Japan

The privacy law

The Japanese government followed a policy of self-regulation for the private sector, especially relating to electronic commerce, until 1999 when lawmakers started working on the Personal Information Protection Bill. After vigorous community debate including from the media, the Bill was submitted to the Diet (the Japanese Parliament). However continued criticism by media groups and opposition parties resulted in the bill being repealed in December 2002. The bill was revised again in response to public criticism that it would, among other concerns, violate freedom of the press. In response to criticism from opposition parties and the media, the ruling coalition dropped the contentious "five basic principles" from the bill and provided exemption clauses for the press. Broadcasters, newspapers, news agencies and other reporting organs, including individuals and writers are exempted from the application of the clauses. The Personal Information Protection Act 2003 Law No. 57 (PIPA) was passed and enacted on 23 May 2003 and came into effect for private sector entities on 1 April 2005.

Although PIPA covers most sectors of the Japanese economy, cabinet ministers are in charge of implementing PIPA in the particular industry sectors for which they have responsibility. Each minister is authorized to issue recommendations or orders to businesses dealing with personal information. Those who refuse to follow ministers' orders could face up to six months in prison or a fine of not more than 300,000 yen. Implementing guidelines have been issued by the Ministry of the Economy, Trade and Industry (METI), the Ministry of Health, Labor and Welfare (MHLW), the Financial Services Agency (FSA), the Ministry of Finance, the Ministry of Internal Affairs and Communications, the Ministry of Land, Infrastructure and Transport, and the Ministry of Justice.

In addition to the media, a government ordinance exempts from coverage an entity that on any day in the past six months maintained and used in its business operations records relating to less than 5000 identifiable individuals. The Act also exempts religious, academic and political organizations and those conducting literary work.

PIPA draws upon the OECD principles. It lists the duties of business. These cover, in broad terms, the matters covered by the OECD principles regarding collection, notification, use, security, disclosure, access and correction.

¹ Information about this review can be found at <http://www.alrc.gov.au/inquiries/current/privacy/index.htm>

Impact of the law

PIPA is quite strongly based on requiring explicit consent from the individuals involved, especially for use of personal information and disclosure of personal information to third parties. The law does provide for some exceptions but these are narrowly framed and appear to have caused considerable confusion about how these work. Some entities were interpreted the law too narrowly. A growing number of businesses refused to lawfully share personal information with public officials and others, for fear of violating PIPA. As a result, a number of socially beneficial uses of personal information had become unnecessarily restricted or discontinued since PIPA came into force. The press reported that a number of Ministries needed to issue clarifying guidance about how the law operates in relation to school emergency contact lists and other normal school activities and also disclosure of personal information for the recall of defective products.² There also appeared to be a gap between consumer expectations of how the law should apply to marketing, and how it actually applied.

To address these misunderstandings, the Cabinet Office held meetings around Japan aimed at assisting members of the public and businesses to gain a clearer understanding of the purposes of law and to apply a common sense approach to applying PIPA.³

A number of businesses were concerned that this kind of education and guidance should have been provided well before the PIPA came into effect for business.

It would appear that the many different guidelines issued by the various Ministries make compliance overly complex for many businesses.

Despite some consumer groups expressing concern during the drafting of PIPA that the absence of an independent data protection authority might reduce the use of enforcement tools, agencies began to enforce PIPA very soon after it came into operation. The reported activity appears to have been unevenly distributed between the various sectors. The Financial Services Agency has issued two warnings, each to major banks in the twelve months since PIPA came into effect, and engaged in at least two major oversight activities, also in the financial services sector. The Ministry of Internal Affairs and Communications has also issued two warnings. However there does not appear to be reports of similar activity by the other Ministerial agencies with enforcement and oversight responsibilities.

The Japanese Cabinet Office is conducting a review of PIPA and has been holding hearings with stakeholders to hear what they think of the law. The task force's main focus for work is the 'overreaction' to PIPA. Issues raised so far at hearings include that PIPA is overly protective and is not serving the real interests of consumers.

There are no specific provisions applying to transfer of personal information outside of Japan. The general rule relating to disclosure to third parties applies and the same quite strict approach to consent applies.

As in Australia, PIPA does not appear to have adequate provisions to deal with globalization and the need to protect information as it travels around the world.

² See for example (<http://www.yomiuri.co.jp/dy/national/20060226TDY03003.htm>)

³ See for example, "Cabinet holds explanatory meetings on the Personal Data Protection Act," Yomiuri Shimbun Tokyo Evening Editions, December 1, 2005 as cited in JPR Newsflash, April 27 2006, <http://www.privacyexchange.org/japan/japanindex.html>.

Conclusions and Lessons Learned

These case studies provide a number of lessons that have implications for any economy seeking to develop and implement a new privacy system. These lessons will benefit business and also consumers from both a domestic and international point of view.

Consistency and simplicity

Privacy law works better for both business and consumers if the law is as simple as possible. This means the law itself should be principles based and as easy to understand as possible for business and consumers. They should be flexible enough to take into account the way most sectors of the economy operate. In many ways privacy is a matter of commonsense and respect for the interests of the customer or citizen concerned. The principles should reflect as much as possible the nature of this common sense. Once this is grasped, implementing the principles is easier and there is less need for detailed official guidance about how to implement them. No law can be sufficiently comprehensive to cover the varied operations of the kinds of businesses to which the law will apply.

If more detail is required, guidelines can be useful, even if only as examples of how to apply the principles in a practical way.

The law should be as comprehensive as possible. This means that the law should cover as many organizations, both public and private sector, as possible. Also, there should be one core privacy law or as few privacy laws as possible. It might be tempting to have separate specific laws for each industry sector and for government, (or public sector) agencies. However this often does not work well because many businesses operate across a number of industry sectors. Where governments outsource functions to private sector organizations, many businesses may handle personal information for government agencies. If privacy laws are segmented between industries and between private and public sector, businesses must look at a number of different laws to ensure they are compliant. The approach taken in the law for each industry sector may not necessarily be consistent and this makes it even more difficult to comply with the laws. The fewer the number of laws, the more consistent the law will be and the less expensive it is for businesses seeking to implement privacy law.

Having comprehensive law also means that there should be few exemptions from the application of the law. There are some very common exemptions among most economies. These include the media and political parties. In developing new privacy laws, it is very tempting to further limit the application of privacy laws in response to pressure from a range of interest groups. However, attempting to limit the application of privacy law further only adds to the complexity of the law without necessarily creating the best outcome for those exempted. In Australia for example, the small business exemptions may have done very little to benefit small business. It also required large business, to which the law does apply, to put in place additional contractual and compliance measures with their small business partners. The exemption has caused uncertainty for many businesses about whether the law applies to them or not. Similarly, exempting the handling of employee records for employment purposes has not reduced the impact of privacy law on businesses as much as those proposing it might have hoped. This is because it is not so easy to separate out employee records from other records businesses hold, and to which the Privacy Act does apply. Also, despite the exemption, employees expected to have their information protected. As a result, other laws were brought in by State and Territory governments to fill the gap. This has further added to the complexity of privacy law in Australia for business.

Early education and guidance

In both Australia and Japan, businesses were concerned that they did not have enough time, between when laws were passed and when they came into effect, to prepare themselves to

comply with the new privacy laws. Guidelines that gave business more detail about how to comply were only provided just before they were required to comply. This led to a considerable amount of uncertainty and anxiety. It also meant that some businesses were not prepared when the law came into effect. This was not necessarily the fault of the agencies required to provide the guidance and education. Preparing education and guidance takes considerable time and resources. The key is to give businesses and the agencies responsible for providing guidance and education, adequate resources and adequate time to educate business and prepared guidelines before business must actually comply with the law. However, ongoing education and guidance is also needed.

Single independent enforcement body

It is also better if there is only one main privacy enforcement body. If that is not possible, there should be a single interagency body for enforcement purposes. We saw in Australia that businesses do not like having a number of bodies within Australia that are responsible for enforcing privacy law. Having one main enforcement body, or an interagency body, makes it much easier to have a consistent approach to enforcement of the law, particularly for businesses that are operating across multiple jurisdictions and multiple industry sectors, as is the trend in economies today.

Having an enforcement body that is independent from the bodies that make the policy and the law is also important. Such a body is able to take a balanced approach to enforcing the law free from political or industry sectoral pressures. The Office of the Privacy Commissioner is separate from Government agencies or ministries that developed and ensured the Privacy law passed through parliament. It is generally seen to be a credible and fair complaints handler by Australian business. The main concern from Australian business about the Australian Office of the Privacy Commissioner is that it lacks the necessary resources to fully exercise its functions. This has meant that both business and consumers have been confused about how the law actually operates.

On the other hand, in Japan, the government ministries that are responsible for developing the policies and the privacy law are also responsible for enforcing the law. This could lead to a less objective view of whether the law is working or not. It could lead to political or other pressures determining whether or not the law should be enforced in a particular case. It may also mean that enforcement is less of a priority in the face of other more urgent affairs of state. Although there has been some enforcement activity in Japan it appears to have been focused mainly on the financial sector and on a few, very big, organisations.

Another advantage of having a single enforcement body is that it makes it much easier to develop a global approach to enforcing privacy law. It means that there is one main point of contact for overseas privacy enforcement bodies and for business needing to coordinate their approach globally.

Importance of global approach

In developing privacy law, governments must look beyond the domestic requirements of business and consumers. Issues that should be considered include having domestic law that is consistent with global norms and which enables cooperation to facilitate safe transborder flow of personal information.

Today, flows of personal information can be rapid (or instantaneous), cross between the jurisdictions of many economies and be part of very complex transactions.

There is widespread recognition that a widely accepted and practical international standard of privacy protection is needed if e-commerce is to flourish.⁴ The importance of this is a key reason why APEC has developed a Privacy Framework. This framework has nine main principles which are intended to provide a basis for moving to a more harmonized approach towards privacy in Asia Pacific economies.

The APEC Privacy Framework is also intended to address the privacy of personal information when it moves between APEC Member Economies or is accessible in more than one economy. Indeed, the seriousness of intent among Member Economies is best seen in the following extracts from Part B of the APEC Privacy Framework:

44. Taking into consideration existing international arrangements and existing or developing self-regulatory approaches (including those referenced in Part B. III., below), and to the extent permitted by domestic law and policy, Member Economies should consider developing cooperative arrangements and procedures to facilitate cross-border cooperation in the enforcement of privacy laws.

.....
46. Member Economies will endeavor to support the development and recognition or acceptance of organizations' cross-border privacy rules across the APEC region, recognizing that organizations would still be responsible for complying with the local data protection requirements, as well as with all applicable laws. Such cross-border privacy rules should adhere to the APEC Privacy Principles.

47. To give effect to such cross-border privacy rules, Member Economies will endeavor to work with appropriate stakeholders to develop frameworks or mechanisms for the mutual recognition or acceptance of such cross-border privacy rules between and among the economies.

48. Member Economies should endeavor to ensure that such cross-border privacy rules and recognition or acceptance mechanisms facilitate responsible and accountable cross border data transfers and effective privacy protections without creating unnecessary barriers to cross-border information flows, including unnecessary administrative and bureaucratic burdens for businesses and consumers.

In 1998, when endorsing the 1998 Blueprint for Action on Electronic Commerce, APEC Ministers acknowledged that the benefits of electronic commerce cannot be received without government and business cooperation "to develop and implement technologies and policies, which build trust and confidence in safe, secure and reliable communication, information and delivery systems, and which address issues including privacy...". The lack of consumer trust and confidence in the privacy and security of online transactions and information networks is one element that may prevent member economies from gaining all of the benefits of electronic commerce.

A recent press release and guidance published by the Office of the Information Privacy Commissioner in the United Kingdom indicates the importance that some economies are placing on protecting personal information when it is outsourced overseas.

Deputy Commissioner David Smith said: "It is becoming more and more prevalent for companies to outsource some of their data processing functions to other companies, quite often overseas. There have been several highly publicised instances recently which suggest that personal information is not always held securely. Companies considering

⁴ The underlying reasons are developed further in "APEC Privacy Framework: Facilitating Business and Protecting Consumers Across the Asia-Pacific" in APEC E-Newsletter Vol 7, January 2006, online at: www.apec.org/apec/enewsletter/jan_vol7/onlinenewsd.html

outsourcing must ensure that they choose companies that can be relied upon to take proper care of the personal information they are entrusted with. Further, they should put in place mechanisms so that when the personal information has been outsourced they can check that it is being properly looked after.

“The Information Commissioner’s Office takes the failure to take proper care of personal information very seriously, and we will not hesitate to investigate where companies have failed to fulfill their obligations under the Data Protection Act. Such investigations could result in formal enforcement action.”

Globally consistent approach

From a privacy perspective, the spread of privacy protection legislation in the Asian region and elsewhere must be welcomed where it is having material effect on improving individual privacy and facilitating trust in modern forms of commerce. However, inconsistencies between these laws make it more difficult for a business to operate across economies in the APEC region as the number of such laws grows. This has the very real potential to reduce the impact of the law in any one economy compared with what is possible with close harmonisation. Europe is already feeling these effects and continues to seek ways of alleviating them. On the other hand, individual economies will continue to address data protection in ways that they see as appropriate to their circumstances and cultures. Respect for each economy’s approach on these matters has been a key component of the APEC way.

More specifically, mechanisms have to be found that ensure that when more than one jurisdiction is involved, the personal information neither suffers from more and more rules applying to it nor loses any of the protection it had when it was first collected. In other words, consistent with APEC Privacy Principle 9, accountability follows the data – no more, no less.

As we saw in both Australian and Japan, privacy law has been developed with insufficient consideration of what might be necessary to achieve global enforcement of privacy law. They are not alone in this. Very few other privacy laws have considered the need to include mechanisms in the law to facilitate global cooperation of privacy laws. There is no doubt that economies will need, very soon, to consider changing their laws to achieve this.

As outlined earlier in this paper a number of Asian economies are thinking about developing new or more comprehensive privacy law. This could be a critical point at which China, in developing its own law, takes a strong leadership role in developing a scheme that harmonises with world trends and which could be influential in the outcomes of these developing laws. An economy that is developing new law now is also in a very strong position to build in mechanisms for global cooperation from the outset. These also could become a model for other economies developing their law to follow. An example of a country taking on this role is that of the Spanish data protection commissioner and the significant role he has played in the development of privacy law in South America.

Measures that a economy can take to put itself in the best position to address global privacy issues include:

- having a principles based approach which aims to align the law as much as possible with principles already developed internationally – the APEC privacy framework would be a useful starting point
- having a single independent privacy enforcement body (or interagency body) as a point of contact for other economies
- giving the enforcement body the power to cooperate with enforcement bodies in other economies.

Enforcement of privacy law globally is the aspect where APEC Member Economies still have the most work to do. In the near future at least, this will have to be developed in the context of existing or imminent domestic privacy and other law.

List of Additional References

"APEC Information Privacy Framework (review, impact, and progress)" APEC Symposium on Information Privacy Protection in E-Government, Hanoi, Viet Nam, 20 February 2006
<http://www.iispartners.com/hanoi.pdf>

"APEC Privacy Framework June 2005 Domestic Implementation", Paper 2005/ECSG/SEM/003 presented to the 1st Technical Seminar and online at:
www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0101.File.v1.1

"Ministers Approve APEC Privacy Framework to Strengthen E-commerce and the Protection of Personal Information, Busan, Korea, 16 November 2005, online at:
www.apec.org/apec/news_media/2005_media_releases/161105_kor_minsapproveapecprivacyframewrk.html

The "APEC Privacy Framework" as endorsed by Ministers in November 2005 is online at:
http://203.127.220.112/content/apec/news_media/2005_media_releases/161105_kor_minsapproveapecprivacyframewrk.downloadlinks.0001.LinkURL.Download.ver5.1.9

The "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" endorsed by the Council of the Organisation for Economic Co-operation and Development (OECD) in September 1980 are available online at:
www.oecd.org/document/18/0,2340,en_2649_34255_1815186_119820_1_1_1,00.html

"An Overview of the Principles Established by the APEC Privacy Framework" Paper 2005/ECSG/SEM/006, presented to the 1st Technical Seminar and online at:
http://www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0104.File.v1.1

"Internal Privacy Governance Frameworks", Paper 2005/SOM3/ECSG/SEM/010, presented to the 2nd Technical Assistance seminar, online at:
www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0080.File.v1.1

"Issues to be Considered in the International Implementation of APEC Privacy Framework", Paper 2005/SOM3/ECSG/SEM/009 presented to the 2nd Technical Assistance Seminar and online at:
www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0079.File.v1.1

"A Survey of International Data Transfer Provisions in Existing Data Protection Legislation – Case Studies", Paper 2005/SOM3/ECSG/SEM/005 presented to the 2nd Technical Assistance Seminar and online at:
www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0075.File.v1.1

"Light Touch or Soft Touch - Reflections of a Regulator Implementing a New Privacy Regime" -
Annual Governance Network & Regulatory Institutions Network Conference, Australian National
University, Canberra, 8 Dec 2004 and online at:

http://www.privacy.gov.au/news/speeches/sp2_04.doc

Technical Assistance Seminar: Domestic Implementation of the APEC Privacy Framework, 1-2
June 2005, Hong Kong, China

www.apec.org/content/apec/documents_reports/electronic_commerce_steering_group/2005.html#SEMHK

2nd Technical Assistance Seminar on Implementation of APEC Privacy Framework: International
Implementation Issues, 5-6 September 2005, Gyeongju, Korea

www.apec.org/content/apec/documents_reports/electronic_commerce_steering_group/2005.html#SEM

Appendix A

Laws, international provisions, and enforcement in privacy regimes for non-APEC and some other economies

There are a number of economies that have comprehensive privacy regimes and an independent privacy enforcement body. Some of these have specific provisions that impose conditions on the export of data overseas, including that there be a substantially similar or adequate regime in the receiving economy. These include Australia and Hong Kong SAR and Argentina.

Others with comprehensive laws and an independent privacy enforcement body have no specific international provisions, but local companies that export data must comply with privacy law in relation to the transfer and are accountable for the way they handle it while they hold the information overseas. These include Canada, New Zealand and South Korea (although that law is less comprehensive). Japan has sectoral enforcement without an independent regulator, but otherwise fits in with this group of economies.

On the other hand, the law in Chinese Taipei has more limited coverage but allows the various sectoral enforcement bodies to restrict export of data in certain circumstances.

Other economies have laws that range in extent of coverage, but no independent data protection authority and no restrictions on export of data. These include Chile (more comprehensive), Mexico (less comprehensive). The privacy laws of these and other Latin American economies have their origins in the concept of “habeas data”, which expresses the fundamental human right that individuals should know what information government (and in some cases business) holds about them. In practice this means that citizens have a right, very similar to that in the OECD principles, to access personal information an organization holds about them.

The USA stands on its own in that it has no comprehensive national laws, but has some very detailed sectoral laws. Their laws do not specifically address data export, but American companies could be accountable to US regulators for how they handle information abroad through provisions in general consumer law such as the Federal Trade Commission Act.

Other economies have privacy provisions inserted in other laws (for example, cyber crime laws) with limited means of enforcement and no restrictions on export of data. These include China, Indonesia, Philippines and Vietnam. These economies are moving towards having more comprehensive privacy law.

Several have adopted a more self-regulatory approach, for example India and Singapore, with no restrictions on export of data at this stage. Both economies are also exploring the possibility of having privacy law.

Options for encouraging or enforcing privacy principles that are not based on law enforced by a public authority are also being explored in a number of economies. The Singapore government, for example, has sponsored the establishment of an eMerchant Trustmark regime called TrustSg (www.trustsg.com.sg) that includes a commitment to respecting privacy and has encouraged business to subscribe to it.

There are a number of ways that regulators could enforce privacy laws across borders. These include being able to enforce their own laws via investigations they carry out themselves in respect of violations in other jurisdictions and/or the ability to cooperate with investigators in other jurisdictions, for example through the sharing of information.

At least four economies appear to have the authority to investigate complaints about privacy violations committed by local companies overseas or in respect of their citizens in regard to

events that have been alleged to have occurred in other jurisdictions. These include Canada, Australia, USA and possibly New Zealand.

Canada, Australia and New Zealand would appear to be able to share information about a complaint with a similar body in another jurisdiction in order for that body to investigate the complaint, either with the consent of the complainant, or under an exception to the general rule of non-disclosure. The US Federal Trade Commission has some powers in this regard and has formally sought additional powers through a so called SAFE WEB Act which is currently before Congress. The power of the Hong Kong SAR authority to investigate overseas breaches by local companies is uncertain. It would appear that their law would not allow them to share information with a body in another jurisdiction.

In addition to simply sharing information, there are other options for addressing multi-jurisdiction events. New Zealand, for example, has a specific power that would allow it to cooperate in a limited way with another authority. The power of other authorities to do this is less certain, but it appears that a combination of consent by the aggrieved individual and memoranda of understanding might enable this to happen in some cases.

Relevant legislative provisions in a number of APEC and other economies are summarised in the following table.

Economy name	Privacy/Data Protection Law Status
<p>Argentina</p>	<p>Law</p> <ul style="list-style-type: none"> • Comprehensive law based closely on EU model <p>International provisions</p> <ul style="list-style-type: none"> • Restrictions on international transfers of data unless adequate levels of protection – criteria for adequacy similar to EU. • DPA can determine adequacy, but none so far <p>Enforcement</p> <ul style="list-style-type: none"> • Has a Data Protection Authority. • Legal remedies for violations of the law • Companies complying with data transfer restrictions using EU approved methods eg using EU model contracts.
<p>Australia</p>	<p>Law</p> <ul style="list-style-type: none"> • Comprehensive national laws, with National Privacy Principles (NPPs) and privacy codes applying to significant proportion of private sector, Information Privacy Principles (IPPs) applying to Federal Departments and agencies as well as some state laws (all based on OECD principles) • Companies can gain approval of a code to replace the NPPs, which are then enforceable as law; codes must be ‘at least the equivalent’ of the NPP <p>The Privacy Act 1988: http://www.privacy.gov.au/act/privacyact/ Guidelines: http://www.privacy.gov.au/act/guidelines/index.html</p> <p>International provisions</p> <ul style="list-style-type: none"> • Conditions imposed on international transfer by private sector organisations, including that there must be consent, or substantially similar privacy regime <p>Enforcement</p> <ul style="list-style-type: none"> • Independent Privacy Commissioner at federal level and some states enforce compliance <p>Office of the Privacy Commissioner (federal): www.privacy.gov.au</p> <p>Cross-border enforcement</p> <ul style="list-style-type: none"> • Federal Privacy Commissioner has the power to investigate overseas breaches of privacy where it involves personal information about Australians handled by an organisation with a connection with Australia and to require it to pay compensation or take other measures to address any breach. Incidental powers associated with this power might enable cooperation with other relevant authorities. • Federal Privacy Commissioner also has power to investigate breaches of privacy of any natural person (Australian or otherwise), either in Australia or overseas where it involves a breach of the data export principle applying to the private sector, NPP 9. • Sharing information with a DPA or enforcement body in another jurisdiction so that that body could investigate a complaint or enforce the law would require the consent of the complainant.

Economy name	Privacy/Data Protection Law Status
Canada	<p>Law</p> <ul style="list-style-type: none"> Comprehensive national laws, provincial and territorial laws <p>Canadian legislation: http://www.privcom.gc.ca/legislation/index_e.asp Other guidance for business: http://www.privcom.gc.ca/ekit/ekit_e.asp</p> <p>International provisions</p> <ul style="list-style-type: none"> No specific provisions relating to international transfer of data. In the private sector, obligations imposed by PIPEDA apply to Canadian sourced data regardless of where the data is processed. Companies remain accountable for data they send abroad for processing and must use contractual or other provisions to protect it. <p>Enforcement</p> <ul style="list-style-type: none"> Independent Privacy Commissioners nationally and provincially. <p>Office of the Privacy Commissioner of Canada: http://www.privcom.gc.ca/index_e.asp</p> <p>Cross border enforcement</p> <ul style="list-style-type: none"> The Canadian Privacy Commissioner has the authority over local companies to hold them accountable for any PIPEDA violations, regardless of where that violation occurs Complaint could be referred to another jurisdiction for it to handle the complaint with the consent of the complainant. Information could be shared with the other jurisdiction if the complainant shares the information, or if the Office relies on the exception to non-disclosure that applies where it is necessary to investigate a complaint.
Chile	<p>Law</p> <ul style="list-style-type: none"> Constitution recognises general right to privacy Comprehensive privacy rights in Law for the Protection of Private Life <p>International provisions</p> <ul style="list-style-type: none"> International transfers of data are not restricted <p>Enforcement</p> <ul style="list-style-type: none"> No independent DPA Enforcement if by individuals bringing private actions in the courts.
China	<p>Law</p> <ul style="list-style-type: none"> No comprehensive law/regulations Work on drafting comprehensive law has started and released in January to the Govt by the Chinese Academy of Social Sciences (CASS) Indications are that it is tending towards being a combination of US and EU model

Economy name	Privacy/Data Protection Law Status
<p>Chinese Taipei</p>	<p>Law</p> <ul style="list-style-type: none"> • Computer-Processed Personal Data Protection Law only applies to government agencies and a considerable number of specified industries in the private sector and establishes a licensing regime for those entities covered • Bill with expanded scope introduced to parliament – intended to overhaul privacy law and incorporate the APEC privacy framework. • Will have stronger provisions relating to domestic and international implementation <p>International provisions</p> <ul style="list-style-type: none"> • Existing law permits Ministry of Justice and other government authorities who regulate the non-public institutions to restrict international data transfers in certain circumstances, including where receiving economy lacks proper laws <p>Enforcement</p> <ul style="list-style-type: none"> • No separate DPA. Ministry of Justice enforces the Act along with the functional regulators for private sector companies. • Redress includes damages and civil and criminal (including imprisonment) penalties for violations.
<p>Hong Kong-SAR</p>	<p>Law</p> <ul style="list-style-type: none"> • Comprehensive laws and codes of practices (based on OECD principles) <p>International provisions</p> <ul style="list-style-type: none"> • Conditions imposed on international transfer by private sector organisations, including that there must be consent, or substantially similar privacy regime, but legal force of provisions uncertain • Privacy Commissioner has model clauses for data export <p>Enforcement</p> <ul style="list-style-type: none"> • Independent Privacy Commissioner enforces compliance <p>Cross-border enforcement</p> <ul style="list-style-type: none"> • Power of Commissioner to investigate breaches occurring overseas unclear • No exception to non-disclosure that would allow information about a complainant to be shared with another jurisdiction for the purposes of enabling investigation of the complaint in that jurisdiction.
<p>India</p>	<p>Law</p> <ul style="list-style-type: none"> • No comprehensive privacy law, but industry grouping NASSCOM is seeking to implement privacy self regulation in the outsourcing and IT enabled industries supplying services outside India. However current wording would allow it to be adopted by other industries • NASSCOM has developed a self regulatory Blueprint for a Privacy and Data Protection Standards Board

Economy name	Privacy/Data Protection Law Status
	<ul style="list-style-type: none"> • Proposing to mandate the Blueprint in the IT Act. • Principles do not align with international data protection norms (eg OECD principles) • Proposes to strictly enforce compliance with the Standards • Requires members to develop a prescriptive compliance program • Enforced by Spot Check Audit Program by the Standards Board • Government approach remains to be seen – if comprehensive legislation is drafted it is likely to be based on the EU model.
Indonesia	<p>Law</p> <ul style="list-style-type: none"> • No comprehensive law • One broad privacy right provision in the Information Technology and Electronic Transaction Bill (cyber crime legislation) waiting for ratification as of 16 March 2006 • Provisions would require processing of personal information by consent unless other laws vary this.
Japan	<p>Law</p> <ul style="list-style-type: none"> • Comprehensive national law, several guidelines and ordinances based on the law, prefectural and local laws (Being reviewed following considerable reaction, report due July) <p>Japan Privacy Resource: http://www.privacyexchange.org/japan/japanindex.html</p> <p>International provisions</p> <ul style="list-style-type: none"> • No specific rules on international transfer of personal data, but the law imposes strong consent-based requirements on all transfers of personal data regardless of location of recipient • Some guidelines make businesses accountable for actions of delegates regardless of where they reside and regardless of having obtained consent <p>Enforcement</p> <ul style="list-style-type: none"> • Responsible ministries/agencies enforce based on guidelines published that they are each expected to produce • Redress can include fines <p>Cross-border enforcement</p> <ul style="list-style-type: none"> • The Japan Information Development Center has entered into a joint venture with BBBOnLine to develop reciprocal online privacy seals that will be as easily recognised by business and consumers located in the United States as those in Japan. This is a self-regulation tool for privacy protection that operates across borders. • Bill introduced in February 2006 that would allow Japanese consumers to file a lawsuit in a Japanese court against a vendor overseas.
Malaysia	<p>Law</p>

Economy name	Privacy/Data Protection Law Status
	<ul style="list-style-type: none"> • Drafted a comprehensive national data protection bill (may be similar to the Hong Kong Personal Data Privacy Ordinance) • The bill includes appointment of a Commissioner • Handling of personal information in the bill is on opt-in basis and consent from data owners before transferring overseas
Mexico	<p>Law</p> <ul style="list-style-type: none"> • Data protection law only applicable to the government • Mexican Federal Consumer Protection Law includes provisions that give consumers the right to restrict transfers of their data for targeted marketing • Currently drafting a data protection bill that includes an appointment of a Commissioner – bill most favoured to get implemented is based on the EU model and includes ADR clauses.
New Zealand	<p>Law</p> <ul style="list-style-type: none"> • Comprehensive data protection law covering public and private sector • Privacy principles generally follow the EU data protection model <p>Privacy Act 1993: http://www.privacy.org.nz/legislation/1993028/toc.html</p> <p>International provisions</p> <ul style="list-style-type: none"> • No specific provisions regarding transfer of data overseas • Principles apply to information held or processed by a New Zealand organisation overseas <p>Enforcement</p> <ul style="list-style-type: none"> • There is an independent Privacy Commissioner <p>The Office of the Privacy Commissioner: http://www.privacy.org.nz/top.html</p> <p>Cross border enforcement</p> <ul style="list-style-type: none"> • New Zealand companies are accountable in New Zealand for compliance with the New Zealand privacy law requirements regardless of location • Privacy Commissioner has some power to cooperate with an overseas DPA • Information could be shared with an overseas DPA in order for that body to investigate a complaint either with the consent of the individual, or on the basis of some exceptions to non-disclosure provided for in the law.
Philippines	<p>Law</p> <ul style="list-style-type: none"> • No comprehensive national laws (provisions in a range of existing laws) • Currently developing data protection guidelines for the private sector • Guidelines include a system for accreditation of data protection certifiers

Economy name	Privacy/Data Protection Law Status
Singapore	<p>Law</p> <ul style="list-style-type: none"> • Voluntary private sector model code – Model Data Protection Code. • Interagency working group considering whether legislation necessary or desirable • Looking at Canadian and Australian models • Provisions being considered include an opt-out rule, a ‘name and shame’ approach • Main DPA may be the Competition Commission of Singapore <p>Enforcement</p> <ul style="list-style-type: none"> • Infocomm Development Authority of Singapore has encouraged the development of a national trust mark programme known as TrustSg www.trustsg.org.sg to facilitate online commerce. Bearers of the trust mark are expected to comply with requirements of the Modal Data Protection Code. TrustSg is a member of the Asia Trustmark Alliance, which in turn is a member of the Global Trustmark Alliance, www.globaltrustmarkalliance.org • About 300 private sector and about 50 public sector organisations have been accredited (as at April 2006).
South Korea	<p>Law</p> <ul style="list-style-type: none"> • Existing national law only applicable to certain industries • Principles based on fair information principles • Currently drafting a restrictive data protection bill applicable to all industries <p>International provisions</p> <ul style="list-style-type: none"> • No specific provisions relating to transfer of data overseas. Data can be transferred if it is in compliance with the law. Consent is required for trans-border data flows within a corporate group. The company remains responsible to the data subject and the data protection authorities <p>Enforcement</p> <ul style="list-style-type: none"> • Currently compliance is enforced by the Personal Information Dispute Mediation Committee which is supported by the Korea Information Security Agency
Thailand	<p>Law</p> <ul style="list-style-type: none"> • Draft comprehensive national data protection bill under inter-agency review • Public consultation to be done soon (as of April 2006)
U.S.A	<p>Law</p> <ul style="list-style-type: none"> • No comprehensive national laws, but sector-specific laws, state laws, and Federal Trade Commission law/regulations • Individuals also have powers to enforce in some cases <p>International provisions</p>

Economy name	Privacy/Data Protection Law Status
	<ul style="list-style-type: none"> • Laws do not address trans-border data flows directly • Legal requirements must be addressed in any business relationship local or international <p>Enforcement</p> <ul style="list-style-type: none"> • Laws are enforced by a range of Federal and State regulators and they have broad powers to enforce them <p>Cross-border enforcement</p> <ul style="list-style-type: none"> • Companies are accountable to US regulators regardless of location, for example, in relation to deceptive representations about privacy and security • In March 2006 the US Senate approved legislation designed to give the Federal Trade Commission greater flexibility to cooperate with foreign counterparts in fighting internet fraud, including spam and spy ware. This includes the power to share information with foreign agencies involved in criminal law enforcement on these issues.
Vietnam	<p>Law</p> <ul style="list-style-type: none"> • No comprehensive national laws • Privacy provision in the Electronic Transaction Law (2006) covers protection of data messages and confidentiality in electronic transactions • Implementation still to be settled