# Economic benefits drive privacy in Asia

At the Annual Privacy Commissioner's conference in September, Hong Kong's Privacy Commissioner, **Raymond Tang**, outlined data protection developments in the Asia-Pacific region. Report by **Merrill Dresner**.

Given the collectivist culture of many Asian economies, there has been less of an association between privacy rights and human rights than is the case in the West, and indeed some Asian constitutions have no provisions at all which recognise the right to privacy. In the Asia-Pacific region, not many jurisdictions have enacted privacy laws or established regulatory systems on personal data protection, although many, such as Malaysia and Thailand, have commenced initiatives, and draft laws are in the pipeline.

However, nations and economies in the region are no less developed in terms of usage of modern technology in electronic communication, and no less impacted by the issues faced by their Western counterparts, specifically spam and unsolicited e-mail, electronic surveillance, the expectation of their citizens with regard to the protection of personal data in cross-border situations, and so on. Asia-Pacific nations and economies quickly came to realise the significance of data privacy as a prerequisite to securing e-trust and e-confidence on the part of e-consumers.

It must be clearly stated that the drivers and the approach to dealing with privacy issues in Asia, have not necessarily replicated the old European privacy traditions. There are some complex reasons for this. In the OECD world, a data privacy framework was established prior to the impact of the Internet and the issues associated with the inter-connected world. In most of the Asia-Pacific jurisdictions, that process was in the reverse order - technology 'hit' them first and then came the realisation that something had to be done to deal with the problems that followed. The approach to privacy, therefore, has tended to be one that seeks to address a particular problem or mischief that has been identified in society, such as computer crime. The incentive to put in place a framework of data protection mechanisms, whether through legislative enactment, self-regulatory measures or a combination of both, is therefore, most frequently cited as economic values and benefits.

## Data protection in Hong Kong

Just as the British approach to data protection reflected its European history, the historical legacy of Hong Kong has been a factor in its closeness to the developing Asian model. Hong Kong, a Peoples Republic of China Special Administrative Region (SAR), with strong links to all the economies in the region, has an OECD-style data protection framework. The privacy law applies to personal data recorded in manual or electronic format. The same provisions regulate both private and public sectors. The system has functioned well and enjoys a high level of public recognition and confidence. The Privacy Commissioner as a statutory body is assured of its independence by the Ordinance (law).

As a member of the family of Asia-Pacific economies, Hong Kong feels obligated to contribute to the regional effort to review the state of play in the context of the region and its diversities in social, cultural and economic backgrounds.

## Asia-Pacific Economic Cooperation (APEC)

APEC consists of 21 member economies. They are referred to as 'economies' because the APEC cooperative process is concerned with trade and economic issues and members engage with one another as economic entities. The member economies are: Australia, Brunei Darussalam, Canada, Chile, People's Republic of China, Hong Kong China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Russia, Singapore, Chinese Taipei, Thailand, United States and Vietnam.

The primary purpose of this forum is to ensure the continued coordination of APEC e-commerce activities.

In 1998, the APEC ministers endorsed a Blueprint for Action on Electronic Commerce. In February 1999, the Electronic Commerce Steering Group (ECSG) was formed to take the initiative on to the next stage, and a privacy workshop was set up in Mexico City in February 2002. This was followed by a cross-region mapping exercise to identify the data protection measures available in the various economies. Work continued into 2003 when Thailand became the host for APEC with workshops and meetings held in Chiang Rai (February 2003) and Phuket (August 2003). Following Chiang Rai, a Data Privacy Sub-Group was established with the mandate to develop a set of privacy principles and implementation mechanisms. This was chaired by Australia, and included representatives from Canada, China, Hong Kong China, Japan, Korea, Malaysia, New Zealand, Chinese Taipei, Thailand and the United States.

## Asia Pacific Telecommunity (APT)

In response to an inter-governmental agreement, the Asia Pacific Telecommunity (APT) was established in 1979 as a regional telecommunications organisation. The APT operates at the inter-governmental level, principally to nurture the development of telecom-

munication services and information infrastructure throughout the Asia Pacific region with a more specific focus directed towards the expansion of services in less developed economies. In 2002, the APT reported in its feasibility study that it had investigated options relating to privacy guidelines for Asia Pacific countries. Subsequently, it was agreed that the region should write its own privacy guidelines for the benefit of members and non-members alike.

As many of the economies in the region share common membership of APEC and APT, the two forums deal with similar problems regarding privacy protection - eg. inconsistencies of approach towards regulating privacy and low levels of public awareness regarding privacy-related issues. The APT guidelines are intended to establish a minimum standard for the processing of personal information in the region, and to promote trans-border data flow with a view to facilitating e-business and harmonious regional relations. The APT initiative seeks to give recognition to 'Asian' diversities in terms of cultural, social and economic differences, greater reliance on a governmental role and a more communal approach towards data privacy.

### The Asia Privacy Forum (APF)

Data privacy as a regulatory concept has been given less attention in Asia than in the West due in part to a different cultural background which emphasises harmony within communities over individualism. However, advances in information technology (IT) and extensive use of the Internet have greatly increased the risk of privacy intrusion on a massive scale and highlighted the need to address the issue of data protection against abusive conduct on the part of data controllers.

While data protection issues have often been discussed at numerous international conferences, the agendas tend to be of greater relevance to the more developed jurisdictions with advanced IT infrastructure and established data protection systems. Recognising diverse levels of data protection is not conducive to development of cross-border trade, it was considered beneficial to establish a forum for the Asian jurisdictions to:

- share their experience
- better understand the specific issues that confront individual jurisdictions
- identify commonalities in those issues; and
- as far as possible, coordinate efforts to identify solutions to matters of common concern.

Closer regional cooperation has paved the way for the emergence of the Asia Privacy Forum (APF). The present membership of APF includes representatives from Hong Kong (PCO), Japan (Electronic Commerce Promotion Council), Korea (KISA), Macau (Justice Affairs Bureau), Malaysia (Ministry of Energy, Communications and Multimedia), Singapore (Info-Comm Development Authority), Taiwan (Ministry of Justice, Ministry of Economic Affairs, Shay & Partners Advocates) and Thailand (National Electronics and Computer Technology Center, National Science and Technology Development Agency and the Ministry of Science Technology and Environment).

## Case study: Hong Kong's Code of Practice on Consumer Credit Data

The largest sector in the economy of Hong Kong is undoubtedly financial services. It was therefore no small matter to check the problems being highlighted in the consumer credit market, which, if left alone, would have degenerated to a crisis which had the potential to destabilise the entire Hong Kong financial market.

Credit providers argued that they had insufficient information on the exposure of consumer credit borrowers, leading to some poor lending decisions being made. Record numbers of individuals were filing for personal bankruptcy. The financial impact of these developments were that credit providers were forced to demand higher rates - peaking at around 11 or 12 per cent. To correct the situation, Hong Kong's Monetary Authority approached the Privacy Commissioner's Office (PCO) and proposed relaxing the provisions of the Code of Practice on Consumer Credit Data, which restricted the sharing of credit information to so-called "negative data", which is information showing defaulters.

The PCO was pressured into working towards a solution that would involve allowing credit providers to collect much more personal data from their customers, and share it more readily. Credit providers began to prepare "wish lists" of items of personal data they wanted to collect from individual customers. The PCO had the unenviable task of trying to satisfy at least three sets of expectations - the public interest, the personal data privacy interests of the individual, and the credit providers. The financial services sector is the largest in the Hong Kong economy, and the PCO was not unsympathetic to its demands; indeed to be otherwise would have been to disregard the public interest.

A public consultation was a step mandated in the Ordinance. 56 per cent of the 282 responses supported the proposal to permit the collection of personal data, subject to stringent safeguards. The opposition to the amendments made it clear that the PCO would be failing in its mission if it were to allow the collection of any additional data by credit providers.

The dilemma is that in trying to satisfy one set of expectations we may effectively alienate a contrary set of expectations. In using the public interest argument in the consultation document and media interviews, the PCO was held, by some, of being more committed to a nebulous privacy concept relating to the "best interests" of all citizens and subordinating personal data privacy rights of the individual.

### ACHIEVEMENTS OF THE FORUM

An informal meeting was hosted by Hong Kong's Privacy Commissioner's Office (PCO) in 2001, immediately after a one-day conference billed as E-Privacy for Electronic Commerce. In November 2002, the Korean Information Security Agency (KISA) hosted the International Conference on Personal Data Protection in Seoul and concurrently the Asia Privacy Forum was formally established and by popular request KISA assumed the role of secretariat.

Another objective of the APF is to bridge the gap between the proceedings of broader international conferences and the situation on the ground prevailing within the APF jurisdictions. It is also hoped that the Forum will provide a conduit between the region and the rest of the world, and in particular, be of assistance to those jurisdictions that are less advanced or in the process of developing a data protection regime.

In order to start from a common platform of privacy interests, APF members began by documenting local concerns with a view to focusing the work of the forum on specific privacy issues with which members could readily identify. The main issues of common concern include unsolicited e-marketing, workplace privacy, identity theft, misuse of personal data by businesses, and regulatory and enforcement issues.

Working groups on Asia privacy guidelines, spam/e-mail, public awareness of data protection and data protection inventory are in the process of being established and they will lead the work of the APF.

### DEVELOPMENTS IN REGIONAL JURISDICTIONS

The Asia-Pacific nations participating in these regional forums (APEC, APF and APT) are at varying stages of development in relation to data protection. There is a range of factors that might affect such development, from political will to community expectations. Social priorities and resource availability also have an effect upon shaping the privacy model which a jurisdiction may find appropriate, not to mention affordable.

In 2002, the Korea Information Security Agency (KISA) undertook a comprehensive survey of the personal data protection frameworks found in APT member countries. The report, published in August 2002, provides a broad picture of the current status of privacy protection in the region.

### NATIONAL LAWS AND PLANNED LEGISLATION

Several member jurisdictions have enacted comprehensive legislation dealing with protection of personal data. Australia, Hong Kong, Japan, New Zealand and South Korea are examples of these. There are others who are on the road to enactment or planning to introduce legislation in the future, for example, Malaysia, Thailand, India, Bhutan, Maldives and Papua New Guinea.

### PRIVACY PROVISIONS IN SECTORAL REGULATIONS

Other countries in the region that do not have specific privacy legislation do, nonetheless, recognise the need to address the issue in their general legal frameworks and have introduced 'privacy' provisions in their sectoral regulations. For example, India regulates wiretapping through a sector specific law on telegraphy. The presence of a large number of call centres in India might have played a part in persuading the Indian Ministry of Information Technology to commence drafting data protection legislation. Bhutan and Laos impose varying degrees of responsibilities on Internet service providers.

### CODES OF CONDUCT

Others, who have established specific privacy legislation, have sought to strengthen or give practical effect to statutory provisions by issuing guidelines or codes of practice to assist industry sectors. Australia, Hong Kong, Korea and New Zealand provide good examples of this approach. Japan, which, until May 2003, did not have privacy legislation specifically targeting the private sector, has also made extensive use of self-regulatory guidelines to promote compliance (see *PL&B International*, May/June, p.15).

### PRIVACY AND HUMAN RIGHTS

It may be that the Japanese experience is symptomatic of the difficulties faced by jurisdictions seeking to introduce privacy legislation for the first time. Data privacy, as an aspect of human rights, means different things to different people in different cultures at different times. Over the past decades, human rights as a concept has acquired a certain flavour - one that may not be entirely compatible with the diverse cultural backgrounds of the region. Nations in the 21st Century, particularly developing nations, have been made to feel the weight of external influence, and, at times, those exercising the influence may have their own agenda. Different forces are at play, both within and outside a jurisdiction. Authorities of the day must balance the competing interests. A driving force is to be found to take the exercise forward, and that driving force is the economic value inherent in the process of free flow of information in a globalised world. It may be fortuitous that that phenomenon has resulted in the realisation of the need to harness that value by way of establishing a framework of personal data protection.

### DATA PROTECTION PRINCIPLES

Several APT member jurisdictions have established personal data protection principles which set out the rights of data subjects and delineate the responsibilities of data collectors or controllers. These principles may be applied in dealing with data privacy issues as diverse as mergers and acquisitions and the regulation of children's personal data. These jurisdictions include Australia, Hong Kong, Japan, South Korea and New Zealand.

### REMEDIES AND DISPUTE RESOLUTION

Those jurisdictions that have established data privacy principles tend to have mechanisms in place for dealing with disputes or dissatisfaction with the local regulator's decision on a complaint. These jurisdictions include Australia, Hong Kong, South Korea and New Zealand. Methods for dealing with dispute resolution vary. A quasi-judicial route, such as by way of an appeal to an administrative tribunal, is available in Hong Kong. South Korea favours mediation and supports it with an efficient operational structure within KISA. Hong Kong also employs a mediatory solution in handling complaints, although mediation is not a statutory function under our Ordinance. The finding of a contravention of privacy requirements under our law may also give grounds for a civil claim for damages which may include injury to feelings.

Hong Kong, South Korea and New Zealand are among those who provide protection to data subjects not resident in their jurisdictions.