4th IAPP Privacy and Data Security Summit and Expo

Developments in Privacy

A View from Asia ~ Laying the Foundations for a Consolidated Approach towards Privacy to meet the Challenges ahead

Thursday 19th February 2004
Washington Renaissance Hotel, Washington - DC

Keynote Address presented by

Raymond Tang

Privacy Commissioner for Personal Data,
Hong Kong SAR, China

個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data

Table of Contents

1 An Overview of Recent Privacy Developments in the Asia Pacific Region

1.1 The development of privacy-conscious societies in the Asia Pacific region has generally followed a bi-modal pattern. Jurisdictions such as Australia, New Zealand and the Hong Kong Special Administrative Region ("the HKSAR") may be regarded as having spear-headed the development of privacy legislation and associated regulatory regimens. The adoption of a regulatory framework in these jurisdictions had at least three major consequences.

1.1.1 Firstly, and most significantly, it established the concept of privacy as a human right thereby extending those rights. This resulted in conferring privacy rights upon citizens of the community designed to explicitly protect their personal data or information.

1.1.2 Secondly, it resulted in the establishment of regulatory regimens that institutionalized privacy protection and provided for a system of redress.

1.1.3 Thirdly it has made society in general more aware of the need to have regard to privacy both within their borders as well as in the regional and international context.

The ultimate goal of those of us concerned with advancing and protecting privacy is to work towards the creation of a privacy-conscious community that respects and invests in the value of privacy as it would, for example, the value of the environment.

1.2 With time it became evident that privacy concerns, and the need to address them, were not some passing social fashion. Certainly by the mid 1990s, and more especially over the last two or three years, there has been a significant boost, a second wave if you like, in broadening the basis of the appeal of privacy in the Asia Pacific region. In part this has been due to ASEAN countries such as Thailand and Malaysia electing to take up national privacy initiatives of their own. These efforts have been supplemented by those of APEC which has brought the topic of privacy to the fore thereby giving added impetus to developments at the national level. For example, relatively recently APEC took the decision to place privacy on the agenda with a view to establishing a set of privacy principles and protocols for its twenty-one member economies to adopt. I shall review this and other developments in rather more detail later on.

1.3 Many of the Asian jurisdictions that comprised what I have termed the second wave of privacy in the region have had the benefit of looking at the merits and features of European model(s) of privacy. There can be little doubt that the traditions associated with those models, based as they are upon the seminal work of the OECD, have set the benchmark in several Asian jurisdictions that have had strong historical ties with Europe. Certainly, in the case of Hong Kong, the European model has shaped our regulatory regimen. In certain aspects, our legislation, the Personal Data (Privacy) Ordinance ("the PD(P)O") has perhaps gone further than some of our colleagues in terms of the protections afforded the citizens of Hong Kong. The PD(P)O contains a detailed set of provisions that not only enshrine the letter and spirit of the OECD principles but take privacy protection to new levels in the region. For example, our Ordinance is universally applicable and does not discriminate in favour, or against, individuals or organizations irrespective of size or sector. It is a robust regimen that accord considerable powers to the regulator, the Privacy Commissioner. I believe that it might have gone beyond giving the OECD principles a dash of Asian flavour. To some extent therefore I regard Hong Kong's privacy regimen as European inspired but locally oriented, rather than simply a direct copy of what has gone before. Of course, that which suits Hong Kong may well not suit another jurisdiction, and certainly we have not devised some universally applicable model. However, the substance of our regimen places us in good stead to share our experience with colleagues in the region[1].

1.4 I think 'the Asianization' of privacy i.e. a regiocentric approach, has some merits that go beyond protecting national interests, be they social, cultural, legal or economic. Not the least of these is that a more customized approach has gone some way towards popularizing privacy in the region. A tendency towards a localized formulation has the advantage of negating possible ill-will. This could arise by imposing an alien concept that is the product of Western liberal thinking rooted in the fundamental value placed upon human rights. The diversity that is Asia demands more subtle and sympathetic arguments that reflect national sensitivities.

1.5 It is also worth recalling that the world was a very different place in the 1980's when the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data were published. I venture to suggest however that in spite of the collective wisdom brought to bear in

[1] In November 2002 the Office of the Privacy Commissioner for Personal Data signed a Memorandum of Understanding with the Korea Information and Security Agency ("KISA"). The express intention of this agreement is to foster better understanding in research into the protection of personal data privacy in the respective jurisdictions.

the promulgation of that declaration few, if any, of the draftsmen could have imagined just how pertinent it would become with advent of PC's, the creation of the Internet and the fixation with cyberspace. Today there is an almost unimaginably vast global information infrastructure that has been central to the emergence and development of E-Business.

1.6 The relatively recent exposure of many countries in Asia to privacy has offered one significant advantage, the capacity to look systematically at privacy legislation and principles against the backdrop of a technologically sophisticated environment. Indeed, it is technology, combined with economic considerations, that has been the main driver around an Asian interest in establishing privacy platforms and protocols that will facilitate and promote trade. The shift in trade from the fortress economy to multi-lateralism to globalism has resulted in the realization that there needs to be some commonly-subscribed ground rules in place to facilitate the free flow of information which is critical to the exchange of goods and services. However, the quid pro quo is that the attainment of economic growth in the international arena should not be at the expense of the subjugation of personal data privacy rights. The importance of this is underscored by at least three developments.

1.6.1 Firstly, a number of economies in the Asia Pacific region have enjoyed stellar economic growth for years, China being perhaps the best example. It is apparent that the importance of privacy is understood by the administration but it may take some time before a national infrastructure is in place to regulate data protection[2].

1.6.2 Secondly, there is consensus in Asia that the full potential of E-Business has not been realized. Whilst greater benefits have accrued in the B2B market, the B2C market has lagged behind. This could mean that business opportunities are being forfeited due to concerns of potential E Consumers not being convincingly addressed.

1.6.3 The massive growth in inter-Asian trade, and Asian trade as a percentage of global trade, means that there has unquestionably been the transfer of immense amounts of personal data across national borders. Little, I suspect, is really known about the seriousness with which the privacy dimension of personal data is treated when transferred across national borders and further shared with strategic partner companies or intermediaries in the supply or distribution chain.

[2] Freedom and privacy of correspondence is recognized in Article 40 of the Constitution of the People's Republic of China.

1.7 In drawing attention to these matters I am in no way pointing the finger quite simply because all is not as I would like it to be on my own doorstep. I spoke earlier of the comprehensiveness of the Ordinance that the Office of the Privacy Commissioner ("the PCO") regulates in Hong Kong. What I did not mention was that the section of the Ordinance [section 33] that deals with the transfer of personal data to a place outside of Hong Kong is the only section of the Ordinance that has yet to be brought into effect. There are various reasons for this and we are encouraged by the current APEC initiative to address transborder data flows in the second phase of this worthy project which will focus upon implementation issues. As a member of APEC it would seem rather imprudent for Hong Kong to 'jump the gun' on the matter of trans border data flows and 'go it alone.' At this point we feel that it is best to establish a level privacy playing field so that regional economies can make use of a common protocol. In due course I am convinced that transborder data flows will be given serious consideration by APEC and Hong Kong will give its full support to the outcome of discussions. Given our role as an important financial centre, and with close ties to the Mainland, the 'APEC option' seems much preferable to unilateral action on our part. I am also of the view that it would be divisive for the privacy pioneering jurisdictions of the region to do likewise when we can consolidate views in a much expanded and influential forum.

1.8 Nonetheless, in an environment of global trade characterized by global communication and transfer of personal data the matter is pressing. In Hong Kong we are just about to embark upon a survey of the transborder data flow practices of local and multi-national firms regionally headquartered in Hong Kong. We are aware, of course, that personal data are being transferred around the clock but we do not know much about corporate polices and practices relating to this activity or about the mechanisms and protections recipient subsidiary, associate or third party companies apply to personal data. Clearly we do not want to take any action that would impede the flow of information thereby damaging economic interests and I think my colleagues in APEC would agree with that. But, by the same token, we consider any information free-for-all to be a less than satisfactory state of affairs. Such a climate contributes towards a cavalier attitude towards accountability in the handling and exchange of personal data.

1.9 The accountability aspect is exacerbated in some economies where costs of doing business are relatively high in comparison with other regional economies. To remain competitive Hong Kong has had to focus on high value-added services of which the financial services sector is the best example. However, even in high value-added and professional services sectors businesses have been obliged to adapt their business models to reduce operating costs yet, at the same time, maintain the consistency

and quality of service delivery. What this means for Hong Kong is that activities such as customer servicing, tele-marketing and IT processing have either been outsourced or are now undertaken in Mainland China[3]. It is probable that the practice will continue to expand. Every business that eventually makes the decision to travel down this already well-trodden path, only accentuates the need for the privacy community to institute effective control measures and redress mechanisms.

1.10 I hope that this background to some of the more important developments and privacy concerns in the Asia Pacific region provides an adequate illustration of the privacy context and some indication of the current state of play. My personal view is that given a somewhat piecemeal picture there are strong grounds for using the good offices of APEC as the forum in which to consolidate developments in privacy, assist our colleagues with less developed privacy regimens to construct robust ones, and formulate privacy protocols that obtain broad based support whilst at the same time facilitating the free flow of information for economic purposes. I also hope that once we have leveled the playing field between member economies by subscribing to common protocols we will be able to use these to make *E*-Business more attractive. Ideally, my wish would be to see some effort directed towards establishing some framework of Internet accountability that would ultimately diminish the concerns of those in the B2C marketplace. If that goal could be achieved it would result in *E*-consumers modifying their perceptions and online purchasing behaviours. Not only would this be good for the consumer market place but it would be good for the B2B market as well. The best outcome would be to have a healthy conventional marketplace complemented by a healthy *E*-marketplace rather than the very lopsided configuration we have at the moment.

In Hong Kong, socio-cultural and physical proximity factors greatly influence buyer behaviour. The Internet has been, and continues to be, largely shunned in terms of its online buying capacities. Successive surveys conducted by both the private and public sectors consistently report findings that the Internet is largely a source of entertainment and/or information gathering. Buying online amounts to a minimal amount of total consumer expenditure and this, as survey findings illustrate, is due to a widespread lack of trust and confidence. I suspect that Hong Kong is not alone in this respect. Efforts in both our regional and international privacy communities can, and should, address frequently voiced complaints about the Internet. Such an endeavour is

[3] There is increasing evidence of this activity in Hong Kong with personal data being transferred to Guangdong Province China, which is adjacent to Hong Kong. Naturally the massive transfer of data to call centres or customer service centres offshore gives rise to privacy protection concerns and these need to be effectively addressed.

ambitious and challenging but fortune favours the bold and there is everything to gain.

2 Privacy in the Asia Pacific Region: The Second Wave

2.1 I have alluded to the fact that, with the exception of those jurisdictions that pioneered the establishment of privacy regimens in the Asia Pacific region, the 'privacy' incentive in the second wave has been Internet and *E*-Business driven. Unsurprisingly therefore the emphasis has been technology biased. That is, many economies saw the real value of 'privacy' in a rather different light to those jurisdictions in the region that had essentially adopted the European model some twenty years ago. Viewed through the lens of technology, privacy appeared both as an obstacle and risk to adapting the 'bricks and mortar' business model to one that was conducted online. Of course the Internet was marketed as being virtually boundless with possibilities. Frenetic activity, coupled with high corporate investment in online infrastructure were rushed to market and heralded as one of the most revolutionary features of 20th century business. The bubble burst and disappointed entrepreneurs were left asking themselves what had gone wrong. One of the principal things that had 'gone wrong' was that *E*-Business was a technology-driven development rather than a consumer or market driven-development. In Marketing, the perils of this approach are well know but unfortunately some law of fast forgetting seems to have afflicted business thinking. One only needs to stop and think a moment about the recently retired Concorde. A magnificent technological achievement but the world's airlines shunned it because it failed to solve their problems. Only a handful were made and they were 'sold' to two State airlines funded from the public purse. The analogy may not be precise but there are certainly some common lessons regarding the fallibility of technology to create strong market demand.

2.2 The post *E*-Business bubble led to a lot of searching questions and this, I submit, is where the 'privacy factor' really made its presence felt. That is, unaddressed online privacy concerns emerged as a serious obstacle in the path of extracting economic value from *E*-Business. One of the most trumpeted concepts of the 20th century had effectively been humbled by a factor that weighed a lot more heavily in the thinking of the target consumer than in the thinking of online service providers. An unfortunate oversight at best.

2.3 Undeterred by this setback, governments in the Asia Pacific region see a very real need to remain alert to E-Business developments if for no other reason than that there is the prevalent belief that *E*-Business will, one day, produce massive business revenues. However, some countries in

the region have less well-developed IT infrastructures, fewer IT professionals and much to do in terms of assimilating learning and diffusing that learning to create computer literate societies. The present concern is that less IT sophistication will jeopardize the prospect of remaining competitive once the costs of doing business increase in any economy where, for example, considerably lower labour costs were the primary reason for investing in the first place. It is therefore understandable, given the need to make the rapid advances necessary, that many governments in the region feel there is an urgent need to 'catch up' with the levels of technological sophistication commonly found in the West. Years of internal strife in some countries, and stagnant growth in others, have left respective governments with few options but to devote limited available resources to economic development and raising the standard of living, in some cases from poverty to subsistence or modest sufficiency. To that extent IT-impoverished societies find it difficult to break out of the cycle just as they found it difficult to break out of the poverty cycle.

2.4 'Catching up' has invariably come to mean doing what more affluent economies are already doing although closing the gap is a demanding challenge in less resource-rich economies. Technology-driven initiatives have assumed a new priority because they are regarded as essential prerequisites of future economic growth and societal well-being. Technological prowess has, since time immemorial, been a determinant of the evolution of society and a major source of wealth generation as well as explaining the differences in the relative state of development between societies. Inevitably technological achievement has become a standard refrain in any rendition of national social and economic progress.

2.5 Set against the wish to achieve economic progress, the regulation of personal data or personal information involving its collection, use, processing, security and retention may well be perceived as an imposition upon normal – or what is regarded as normal – economic activity. Different views are held in the region and that among those views is one that regards personal data privacy as something of an irritant or impediment to the free flow of information across national borders. In this regard, economies in the region have to set their own priorities. Hong Kong has made its choice early on and enacted a comprehensive regulatory regime which has done much to re-assure its citizens. In the context of an international business centre, that regime would be familiar to the international business community that come from jurisdictions which pay due regard to personal data privacy - a feature, I would like to think, that indicates sophistication and societal maturity.

2.6 In explaining the thinking behind the perception that the overlay of privacy upon trade is something of an irritation it may well be that a rather esoteric concept such as personal data privacy appears as something of a luxury on the national agenda of a developing economy and can therefore be largely disregarded, at least for the time being. Additionally, the whole notion of trying to get buy-in to the idea that offline data should be regulated may be inherently difficult from a cultural perspective. Personal information is an inalienable aspect of human societies. Collection and use of information about people, whether by government, businesses or private individuals has been going on since time immemorial and is a common and natural thing to do. In some societies, as I have commented, the notion is alien because collectivism, emphasis on social harmony, and a strong cultural belief in taking the middle path is deemed to be preferable.

2.7 However, the combined effect of the economic value of information, the expansion of goods and services offered online by both the private and public sector and the desire to expand trade intra-Asia Pacific and globally have created a new realization that the protection of personal data is a subject well worthy of consideration. Just as those aspiring to membership of the European Union must fulfill certain conditions for membership that frequently mean placing compatible legislation on the statute book prior to being granted full membership, there is now broad recognition in the region that personal data privacy is an issue that must be addressed such that a negotiated minimum level of protection is afforded the individual. Relatively recently, a number of Asian organizations have taken it upon themselves to debate and negotiate personal data/information protocols and I propose to mention a few to convey an understanding of how economies in the Asia Pacific region are taking a concerted approach towards protecting privacy without inhibiting the free flow of information.

3 Current Asia Pacific Privacy Initiatives

Electronic Commerce Steering Group (ECSG)

3.1 APEC established the Electronic Commerce Steering Group (ECSG) in 1999[4]. The primary purpose of this forum is to ensure the continued co-ordination of APEC *E*-commerce activities. In endorsing the 1998 Blueprint for Action on Electronic Commerce, APEC ministers acknowledged that the true potential of electronic commerce could not

[4] 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. All 21 economies are represented on the ECSG.

be realised without government and business co-operation. This was regarded as critical " *...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... "* Surveys of consumers in the region have consistently shown their reluctance to become involved in *E*-transactions and naturally this has impeded potential. In seeking to address consumer anxieties APEC deemed it necessary to develop clear and transparent transborder data protection standards to boost confidence. The mission continues with the next meeting of the ECSG to be held later this month in Santiago, Chile.

APEC Privacy Principles

3.2 A second privacy initiative taken up by APEC involves the bringing together of privacy advocates who have a common interest in working towards the advancement of the region in terms of data protection. The intention is to develop a commonly accepted standard of information privacy and to harmonize differences between member countries. One of the principal aims of the initiative is to restore trust and confidence in *E*-business thereby modifying consumers' perceptions towards online transactions.

3.3 The diversity and richness of Asian cultures reflects in the value attached to privacy and this has resulted in variations afforded the citizens of those countries. Even for those jurisdictions that made an early start the scope of coverage and regulatory powers are by no means uniform. For example, some laws are sectoral on topics - spamming - others are similar to the Hong Kong format with dedicated personal data privacy legislation which enables them to issue codes of conduct to regulate specific privacy issues. Regulatory mechanisms also vary. Some are substantially more legalistic whereas others rely upon self-regulation. Similarly, conflict resolution mechanisms co-exist in forms as different as judicial redress and mediation.

3.4 The sub-group working on this initiative seeks to establish regional guidelines that will go some way towards strengthening members regulatory frameworks either by building a system from scratch or by making an existing system more robust[5]. Of course the exercise is rather more complex than may initially appear because it needs to strike a balance between maintaining the free flow of information and protecting personal data privacy. It also needs to address the issues presented in balancing the public interest and private rights.

[5] The APEC Data Privacy Sub-Group consists of 11 economies: Australia (Chair), Canada, China, Hong Kong China, Japan, Korea, Malaysia, New Zealand, Chinese Taipei, Thailand and United States.

3.5 Early debate by the sub-group sought to establish an appropriate approach. Some members were of the view that territorial limits should not impact on the concept of privacy and accordingly it would be possible to borrow from the European model. However, other members have expressed a preference for a set of principles that more faithfully reflect the characteristics and needs of APEC member countries. While the OECD Guidelines and European Union Directives offered a starting point for discussions my inclination is that a more regiocentric set of guidelines will ultimately emerge in the final drafting. As discussions have progressed the picture that has emerged is that member countries would prefer to think outside of the European 'box'. My view is that this mentality lends freshness to the initiative which should at least be given the opportunity to demonstrate its worth. Currently my colleagues and I are working on version eight of the draft which has benefited from numerous inputs and revisions. Hopefully, the final document will be available before long.

3.6 I remain confident that ultimately the forum will have produced a rubric that upholds the traditions of personal data privacy protection whilst at the same time reinvigorating them. Indeed, it may be beneficial for my colleagues in the European privacy community to review the adopted draft to see if there is any learning to be derived.

3.7 Throughout this project the APEC sub-group has been mindful of the concurrent efforts of the Asia Pacific Telecommunity (APT) in preparing another set of guidelines. Efforts will be made to ensure that there is consistency in the output of these separate endeavours. One suggestion has been to incorporate aspects of the APT Guidelines into the APEC Privacy Principles. For example, those sections detailing national implementation and international cooperation.

At present I think we have arrived at a tentative agreement that will see APEC Privacy Principles as offering core regulatory guidelines at the macro level. That is, a declaration whose substance and intent resembles that of the OECD Guidelines. In contrast the APT Guidelines, at least in their first incarnation, address day-to-day information management and implementation mechanisms. I am sure that ultimately the two documents will be compatible and work in favour of the communal interests of all member economies.

3.8 I should perhaps add that once the APEC Privacy Principles are ratified by member economies the working group will move on to the second phase of the project which is to look into implementation issues and mechanisms. I envisage that this process will generate considerable debate. Member economies are likely to be enthusiastic about signing up to the principles but I suggest that they will need to see a fair amount

of flexibility in the manner in which those principles are implemented within the economies. This will be a challenging exercise but I am confident that the members of the working party will ensure that national integrity and legal systems are not compromised by any implementation protocol.

Asia Pacific Telecommunity (APT)

3.9 In response to an inter-governmental agreement the Asia Pacific Telecommunity[6] ("the APT") was established in 1979 as a regional telecommunications organization. Unlike the APEC privacy forum which is not confined to government officials, the APT operates exclusively at the inter-governmental level. The principal raison d'être of this organisation is to nurture the development of telecommunication services and information infrastructure throughout the Asia Pacific region, with a more specific focus directed towards the expansion of services in less developed economies.

Recognising the inter-relationship between access to information and respect for privacy, the APT undertook a feasibility study that investigated options relating to privacy guidelines for Asia Pacific economies. The survey findings were reported at the 22nd APT Study Group Meeting in August 2002. Subsequently it was resolved that the region should author its own privacy guidelines for the benefit of members and non-members alike[7].

3.10 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, e.g. inconsistencies of approach towards regulating privacy and lower 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 transborder data flow with a view to facilitating *E*-business and harmonious regional relations. It is expected that the synchronization of members domestic regulations will enable them to align with the regional model thereby eliminating the prospect of a "conflict of laws". With common criteria for protection, any undue governmental intervention in the defence of privacy, or other overly restrictive requirements impeding cross border data flows, should be minimised.

The Guidelines, which distinguish between legislative proposals and a Model Code, serve to govern the processing of all sorts of personal information, irrespective of whether it is offline or online. They also

[6] The APT currently has 32 members, 4 associate members and 95 affiliate members.

[7] The project was led by the Korean Information Security Agency (KISA).

apply to both the public and private sectors. The current draft places great emphasis on specificity with extensive provisions relating to data management, for example, the roles of government and the responsibilities of business associations. An Alternative Dispute Resolutions (ADR) process, which is increasingly favoured by member countries, has also been proposed.

4 At the Crossroads ~ Community's Security Concerns

4.1 Events over the past couple of years have left some of us with a feeling that the region might be at a crossroads. We are left wondering what might be our eventual destination. The matter is made more urgent perhaps by the trend we seem to be witnessing which is a gradual but accelerating impact on privacy rights in addressing the community's concerns over terrorism. It would be folly for Asian economies to stand on the sidelines in the face of international terrorism and certainly in the case of Hong Kong we have given solid backing to international initiatives aimed at curbing this deadly menace. However, we are cognizant that in taking strong deterrent measures we may well be creating a climate in which surveillance thrives at the expense of privacy. Given the current state of privacy development in the region, where we are heading at this crossroads may have long term implications on the success or otherwise in establishing a credible regional privacy regime. I would therefore like to digress slightly and look at what appears to be a rather one-sided contest: *Privacy vs. Surveillance*.

4.2 I fully recognize that the threat posed by international terrorism requires drastic action and perhaps unprecedented security measures. I also recognize that national security is non-negotiable. However, I am concerned that privacy may be in danger of not being given due regard in the course of introducing extensive counter-terrorism measures. Without disputing the need to put in place adequate measures, there are divergent views regarding the significance of terrorism as a threat to national security. That is, terrorism is not perceived to be a phenomenon that poses an equal level of threat to all societies. It may be that the latter point goes some way to explaining why something like 50% of UN member countries have yet to 'report in' with an assessment of terrorist threats in their respective countries in response to a UN resolution made in the wake of the 9-11 attacks.

4.3 Disparate perceptions of the level of threat posed by terrorism may well create the conditions that give rise to a conflict of rights. By this I mean the right of the citizen to enjoy a reasonable expectation of privacy (and related protections) will be pitched against the mandate of the State to afford its citizens a level of security that will enable them to live their

lives without the fear of terrorist intimidation. National governments have, for good and legitimate reasons, put in place strong measures that directly impact upon personal privacy. Heightened security alerts will likely affect perceptions and inform opinion surrounding the privacy/surveillance debate. And, if it comes to a battle of wills then the safe bet is that privacy will come in a poor second. Of course 'the contest' I have alluded to begs the question as to whether there *can* be an accommodation of privacy rights in a climate in which both political authorities and popular sentiment accord counter-terrorism measures priority and urgency. To me, one of the fundamental realizations to emerge from the events of 11th September is that personal and national security can no longer be addressed with a light or largely invisible touch. It is something of a cliché but it has been said that the world will never be the same as a consequence of the events of that day. One victim of that changed world has been the integrity of privacy and this may be an inevitable but unfortunate outcome that we have to get used to.

To a certain extent I can grasp that and live with it. However, what is more difficult for the privacy community to come to terms with is the prospect of terminal degeneration of privacy, both as a concept and human right. May be that is the price society will ultimately have to pay for enhanced security but to some it is both a high price and a minor victory for terrorists.

4.4 Should we call it a day then? At this point I don't think the privacy cause has been, or should be, written off because I think it is a potent symbol of contemporary social values which every modern society should aspire. In Asia, as I have demonstrated, we are moving ahead with a number of initiatives designed both to sow the seed of privacy and shore up the privacy gains that have been made. However, in the climate I have depicted that is not going to be easy. I do not think I am alone in believing that even in established privacy regimens privacy rights should any longer be seen as inviolable. The scourge of terrorism has brought privacy issues to the public fore and we need to see this as an opportunity rather than a challenge. The opportunity lies in harnessing public opinion and seeking to dispel the worst-case scenario by moving to consolidate the gains and responding to terrorism with measures that would not eclipse privacy forever.

4.5 At present, as I have tried to convey, there is a good deal of disparity in privacy regimens in Asia Pacific although regional initiatives are making progress towards bringing some order to the situation. Let me give you some of the flavour of the differences that can be discerned when surveying the scene.

4.5.1 Firstly, there are differences in scope. The more comprehensive encompasses all data and is to be contrasted against the sectoral that addresses privacy in the context of telecommunications or perhaps the Internet. The latter approach invariably results in dedicated legislation designed to target the specific issues within a single economic sector.

4.5.2 Secondly, there are application alternatives that inspire privacy legislation that discriminates between sectors. In Hong Kong for example we have resisted this approach and enacted legislation that is universal in its application to the individual and organization irrespective of sector, size, business turnover etc. Having said that it does allow for exemptions such as crime and security.

4.5.3 Thirdly, there are operational distinctions between federal and state legislation. Australia for example has both federal and state privacy agencies. It has also relatively recently extended the application of the law from an exclusive concern with the public sector to the private sector as well, although there is still an exception for smaller enterprises.

Having listed these distinctions I think that there can be little doubt that the search for a universal model of privacy is unlikely to be very fruitful. Given the varying stages in privacy development, the imposition of a 'one size fits all' approach is unlikely to be met with approval. However, I do think that the possibilities outlined provide a range of options that are attractive and, as a consequence, there is some enthusiasm for privacy in Asia. Terrorism notwithstanding, the game is not lost in the region if for no other reason than that in some countries it has hardly begun. I am therefore optimistic that Asia may benefit from the position it is in. Just as rapid advances in IT placed privacy in a new light, so too may terrorism. It should be possible for some countries in the second wave to look at realistic privacy protections set against the experience of international terrorism and resultant security concerns. I think therefore that at this juncture efforts will be redoubled to create a situation in which privacy rights and national security can co-exist. Admittedly, we may have to get used to the fact that some of the privileges of the past have been compromised but this is a lot preferable to throwing in the towel and giving up altogether.

4.6 As I have mentioned the Hong Kong SAR has enjoyed the benefits of a comprehensive regulatory regime where the individual's privacy right is given due consideration. That consideration goes a long way to resist any diminution of those rights that may arise from the influence of 'intervening events' e.g. counter-terrorism measures. The question that

comes to mind is whether it would be prudent to put in place a system now to avoid any lasting damage to the notion of the individual and his private sphere? Or, is that notion no longer relevant given the geopolitics of an increasingly inter-connected world? In Hong Kong we have made our choice but that does not mean we are unaffected by the events of the times and the pressures that arise from those events. Other jurisdictions have also to come to grips with public sentiment and the expectations arising from random events that place privacy issues in the public limelight.

5 The Shape of things to Come?

5.1 I have resisted offering some concluding comments in preference for using this opportunity to outline a possible scenario that could, if left unattended, have the effect of undermining the rationale for a pan-Asia Pacific privacy initiative and the gains made by national privacy regimens within the region. It seems, in a climate in which there are appreciable concerns around national security that there is an almost inevitable pressure upon law enforcement agencies to both collect and collate data on the individual or defined populations of individuals in a wholesale fashion. Not only is there an established infrastructure to facilitate this collection and collation but, rather like the tendency in the commercial marketplace, there is invariably an unwritten law that says the more data collected the better. So, it is quite probable, in my view, that we will witness a sustained need to open up databases in the private sector for inspection by government agencies, possibly with good intent, if not for probable cause. As I have said it is easy to comprehend the case that would be advanced by governments to support the use of such measures, provided we make the assumption that, in the majority of instances, the scrutiny of databases by law enforcement and security agencies *is* a response to good intelligence concerning terrorist activities. In the case of airline passenger manifests there can be no doubt of this.

5.2 However, in responding proactively to the terrorist threat we may be opening a Pandora's box of problems that may have serious, if not irreversible repercussions, not only for privacy interests but for business interests as well. When customers volunteer their personal data through any medium it is reasonable for them to suppose that the purpose of this collection is to enable them to avail themselves of access to goods or services. What if data collected ostensibly for business purposes are to be made available to government agencies acting on intelligence or a hunch or simply as a matter of routine? Would the customer think twice before contributing his data into the pool of information? What we don't know from any longitudinal or cross-cultural surveys is the extent to which this would have a bearing upon community, customer or

individual perceptions towards the legitimacy of such intrusive practices, or how this might affect their spending behaviour. I suspect there would be a range of views from those of implacable opposition to resigned acceptance. A levy, if you will, that the spectre of terrorism has imposed upon the privacy rights of the individual.

5.3 Quite clearly the pervasive use of credit, loyalty, retail and store cards leaves an electronic trail of behaviours that are of immense corporate value. The new battleground is for competitive advantage derived from data, information and knowledge rather than simply the brand's equity. However, the pattern of purchasing I am referring to is less well-established and less sophisticated in some Asian countries where there is still massive growth in the consumer credit market. China being a very obvious example. Nonetheless, there can be no doubt that these economies will follow the path taken by more mature economies a) because the demand is there, b) because more robust financial infrastructures and regulatory measures are in place and c) because credit-based purchases provide marketers with a mechanism for rapidly expanding market demand.

5.4 In more developed marketplaces market intelligence is crucial because markets are often at or near saturation levels. Equally so, market intelligence is crucially important in driving demand in emerging or early growth markets. Of course marketers are not the only ones to realize the value of what is stored in consumer databases. Increasingly it seems that for a different set of motives government agencies understand the potential value of that intelligence. That realization might place management and corporate presidents in a very unenviable position. The personal data of the customer, or the employee for that matter, is invariably collected for reasons that relate to the Marketing and Human Resource activities of the business. Should we now assume that well-intentioned counter-terrorism measures are a legitimate concern that should, in some way, be accommodated by businesses? Sound arguments can be advanced to support the proposition that it is both a patriotic duty and indicative of good corporate governance to permit the scanning of consumer or employee data for such purposes. However, the corporate dilemma I am alluding to would be amplified if there were to be a consumer boycott of policies, no matter how well-intentioned, that opened up this data to scrutiny by government agencies. To me, this doesn't sound like a preposterous interpretation of an overly vivid imagination, but something that may come about, in one manifestation or another; the more so if terrorist incidents intensify. A consumer backlash may well be the consequence of this series of events and if that were the case it would leave businesses between a rock and a hard place.

5.5 Electronic capabilities, and the increasingly international nature of markets lend my suggestion a global dimension. What, if any, would the impact of this be upon the work we have been doing in the Asia Pacific privacy community? My view would be that the situation I have depicted could shake the foundations of our attempts to find a consolidated approach towards establishing privacy regimens in the region. I think a vociferous data protection lobby could emerge in the community and irreconcilable differences would interfere with, if not be seriously detrimental to, business interests. While I do not think the warning bells are ringing just yet I do think that potential storm clouds are gathering. I can see that in businesses where very sensitive market data are collected and collated e.g. the healthcare industry, that there would be tremendous consumer resistance to the scanning of such data by government agencies, irrespective of the threat posed by terrorism. The challenge that lies before us is to be able to develop and sustain privacy regimens that do not impede counter-terrorism work but at the same time do not give government agencies impunity in denying a reasonable expectation of privacy in the community.

Is this the shape of things to come? I leave that an open question but if there is just an element of realism in what I have outlined then I think that the privacy debate needs to assume a new significance on national agendas. It is incredibly important that we have that public debate now so that political leaders better understand the perceptions of the community in terms of the privacy parameters that may need to be established and the benchmarks that are needed to preserve the trust and confidence of the community at large.

Raymond Tang
Privacy Commissioner for Personal Data
Hong Kong SAR, China

19 February 2004
at Washington, DC, USA