25th International Conference of Data Protection and Privacy Commissioners

Practical Privacy for People, Government and Business

10-12 September 2003

Sydney, New South Wales, Australia

Plenary Session A – Regulating Privacy …what others are doing

10th September, 2003

Personal Data Privacy: The Asian Agenda

Presented by

Raymond Tang

Privacy Commissioner for Personal Data,

Hong Kong SAR, China

香港個人資料私隱專員公署

Office of the Privacy Commissioner for Personal Data, Hong Kong

Table of Contents

1 Introduction

1.1 Under the generic heading for the session **"Regulating Privacy; what others are doing,"** I want to develop some views shaped by what may become the Asian model of privacy. While this model is rudimentary it offers those who may be less familiar with pan-Asian initiatives towards privacy a perspective on the approaches that have been engaged in this part of the world to further the cause of privacy protection. Although (what might conveniently be termed) the European model of privacy has been influential in the thinking about establishing privacy regimens in the Asian region, it would seem that the Asian process is not simply an attempt to replicate the European model but rather an exercise to identify a model that best suits the Asian requirements.

1.2 This is perhaps not surprising given the time that has elapsed since the OECD Principles were first articulated and subsequently embraced by those jurisdictions that were in the forefront of the movement to regulate privacy. In the 1980s I think the inclination was to regard the protection of privacy as a responsibility that should be assumed by liberal democratic societies. This was advanced as 'the right thing to do' and further justified on the grounds that it was being done for the right reasons. Added momentum was given to this view by those who conceived of the protection of personal privacy as an essential right of the individual. Ultimately this was elevated to the status of a human right and is still popularly conceived as such in the West.

1.3 To my mind that very brief summary, and I will develop upon it later, is at variance with the evolution of privacy in Asian countries and representative organisations of those countries such as the Asia-Pacific Economic Cooperation (APEC), a trading bloc comprising of 21 economies. I feel this is for a number of valid reasons and that those reasons reflect a rather different way of approaching the regulation of privacy. To give but one example – culture – the tradition in many Asian societies is not to emphasize individualism of individualistic identities or pursuits. The tendency, and of course there is a good deal of variation and richness to Asian cultures, is to place greater emphasis upon collective ideals and harmony. For this, and other reasons, there has been less emphasis and recognition given to the 'human rights school' of privacy. Nonetheless, as we are witnessing, the commitment to privacy protection in Asia is by no means diminished by the alternative nature of the approach.

1.4 I want in this paper to explore two alternative approaches to regulating privacy if for no other reason than to facilitate comparison. In so doing I in no way make any value judgement regarding the respective approaches in terms of which is 'right' or 'wrong', or indeed which is 'better'. My message is simply that the protection of privacy is accorded different values in different societies and those values are reflected in different approaches. In both contexts the European and Asian models seem appropriate. Having said that I must declare a bias which is that, given the recency with which privacy has emerged in Asia, there has been the opportunity to look systematically at the European model in terms of what it has to offer. It should also be noted that the main drivers around privacy in the Asian context are symptomatic of changes that have taken place over the period of two decades. Singularly the most influential of these has been technology and that is likely to remain so in the immediate future. However, there has also been significant economic change, most notably in the relationships in the global economic community, away from a fortress mentality through bi-lateralism and multi-lateralism, towards globalism. These economic developments require the free movement of immense amounts of personal data and recognition of this is reflected in the framing of privacy policies. Certainly this dimension has been instrumental in developing privacy initiatives in Asian jurisdictions.

2 The Early Years – OECD Principles

2.1 In the beginning there were the OECD Guidelines Governing the Protection of Privacy and Trans border Flows of Personal Data. The principles enunciated in this declaration were soon recognised as the very essence of privacy values. They formed a succinct and cogent approach to personal data privacy that was populist rather than extreme in nature. They also provided the benchmark by which those pioneering privacy regimens, such as New Zealand and Australia, would be able to assess the effectiveness of their endeavours.

2.1 It is worth recalling that the world was a very different place in the 1980s and I venture to suggest that the Expert Group under Justice Michael Kirby's chairmanship did not, upon the completion of their work, envisage just how important the protection of personal data would become with the advent of PC's and the impact of the Internet and cyberspace on everyday life. Concepts and terms such as global information infrastructure, a global information society and electronic commerce were not yet in vogue in those days. My recollection is that the raison d'être of the Expert Group was to harmonise national legislation rather than to give substance to more general covenants such

as the ICCPR. The eight 'Basic Principles of National Application' have largely stood the test of time although to some extent that test is being re-examined in Asian jurisdictions today.

2.2 The thinking behind the OECD guidelines is worthy of mention for at least three reasons.

- Firstly, they sought to advance the free flow of information between OECD member countries and to avoid any obstacles that might impede the development of social and economic relations between member countries. This was of primary concern. It was somewhat incidental that the output of the Expert Group was a statement of international expectations regarding the protection of personal information.

- Secondly, the document provided " …a general framework for concerted action by Member countries: objectives … may be pursued in different ways."

- Finally it is evident that the guidelines relate fundamentally to data protection rather than privacy protection per se.

2.3 The reason I mention these three points is because although it is two decades on there is a similarity between the OECD's general observations of purpose and those that have inspired some of the relatively recent pan-Asian initiatives towards personal information/data privacy protection. In particular, the desire to preserve national sovereignty and to legislate in the national interest, rather than to have a personal data framework imposed by an external party, has been uppermost, for example, in the minds of many delegates to the APEC privacy initiative. Just as the OECD acknowledged that there were significant differences between Member countries, APEC has also acknowledged that its privacy initiatives should not operate from the common assumption that 'one size fits all'. As a result there has been a conscious effort not to deny the diversity of cultural, political, legal and social identities of individual member economies. Therein lies one of the real challenges in such a venture, i.e. the ability to obtain broad-based support for any declaration of personal data principles without compromising the jurisdictional integrity of the 21 economies comprising APEC. Not only have my colleagues and I accepted this imperative but I am also pleased to report that we are making solid progress in our collective efforts.

2.4 More recently in January 2003 an OECD working party on Information Security and Privacy issued a document titled ***Privacy Online – Policy***

and Practical Guidance ("the Guidance"). This Guidance seeks to maintain the currency of the OECD Guidelines by looking at them in the context of the information age and network technologies.

On the one hand the Internet and E-business offer massive market opportunities through information exchange which facilitates more accurate consumer segmentation, targeting and positioning. Consumers benefit by being offered products and services that more closely equate with their personal needs. In addition, the information available assists consumers in their decision making processes such as assessing the uncertainties associated with high-value purchases, e.g. a new car. The downside of course is that the very same technologies that offer these benefits have the propensity to track, profile and intrude upon the privacy of the online consumer. A case in point is provided by Hong Kong where online shopping accounts for only around 1% of total consumer expenditure[1].

2.5 The Guidance observed that " …related privacy issues arise from the fact that all this computer-accessible personal information, whether automatically generated or not, can potentially be collected, stored, detailed, individualised, linked and put to a variety of uses in places geographically dispersed around the world, possibly without user knowledge or consent." It subsequently went on to detail a six-step programme for online privacy protection:

~ encouraging the adoption of privacy policies;

~ encouraging the online notification of privacy policies to users;

~ ensuring that enforcement and redress mechanisms are available in cases of non-compliance;

~ promoting user education and awareness about online privacy and the means at their disposal for protecting privacy;

~ encouraging the use of privacy enhancing technologies: and

~ encouraging the use and development of contractual solutions for online transborder data flows.

[1] A survey undertaken by the PCO in 2001 into data subjects attitudes indicated that 'privacy protection' was the most important consideration among respondents when making their decision to purchase on the Internet. It was also found that concerns around 'the misuse of personal data by third parties' was second only to 'money loss due to interception of your credit card details.'

As I mentioned this action plan has been adopted by the OECD as a mechanism for keeping the OECD principles contemporary. Whilst this initiative is laudable I do not think it would be too unkind to say that it is something of a catch-up response to technological developments. The acid test of course remains less in the nature of strategic components of the plan and more in its implementation and effectiveness in promoting compliance.

In contrast, APEC privacy initiatives, which have been less influenced by the Euro model towards privacy protection, nurtured in a pre-digital era of communication and information exchange. Indeed the cyber challenge to the protection of information privacy has been the starting point of APEC and other Asian privacy initiatives.

3 The European Union Directive on Trans border Data Flows ("TBDF")

3.1 Directive 95/46/EC of the European Parliament and Council added further substance to the OECD Guidelines by seeking to remove the obstacles to flows of personal data across the national boundaries of Member states while at the same time affording protection of personal data in the processing and transfer of personal data either between Member states or to third countries. Essentially the objective was to ensure commensurate levels of protection in both Member and third party states by establishing an adequacy test.

3.2 In December 2001 the European Commission drafted a set of standard contractual clauses for the transfer of personal data to parties in non-Member countries. The purpose of the Commission' s decision was:

~ to facilitate the transfer of personal data to a third party country where that country ensures an adequate level of data protection and Member States' laws are respected prior to transfer;

~ to uphold the authorization granted to Member States**,** subject to certain safeguards being in place, to the transfer of personal data to third countries that which do not ensure an adequate level of protection [the safeguards being a constituent aspect of the contractual clauses].

The standard contractual clauses give comprehensive coverage to important aspects of TBDF such as obligations of the data exporter, obligations of the data importer, liability, mediation etc. To that extent

they offer a very practical template that will be of value to organisations such as APEC when they come to debate similar issues.

4 Privacy Protection – The European Model

4.1 There can be little doubt that landmark developments in personal information privacy in Europe were instrumental in establishing privacy regimens both there and further afield. To that extent the Europeans may justifiably be regarded as pioneers of the privacy movement and their contribution has been immense. However, it is recognized that diversity in the history, traditions and institutions of a particular country may be different both in form and substance from those of say another Member state in the European Union. Clearly there has been a need to build some bridges in order to reach agreement upon a common privacy platform with which Member states can subscribe to without feeling that they are in some way compromising their national integrity.

Interestingly, this picture is similar to the situation we are currently facing in Asia. Pan-Asian privacy initiatives are a relatively recent addition to APEC's business agenda but one that is welcomed by constituent member economies. I would like therefore to move on from this brief retrospective look at the origins and developments in privacy in Europe and switch our focus to Asia where, with several exceptions, privacy regimens are at a less sophisticated stage of development.

5 Privacy – The Asian Context

5.1 Developments in privacy protection in Asian jurisdictions needs to be set against the regional backdrop which I will survey in brief.

- Firstly, it must be said that there are considerable differences within the Asia Pacific region in both the approach towards privacy protection and its state of development. For example, Australia and New Zealand provide examples of mature regimens and were in the vanguard of those jurisdictions that legislated for and institutionalised privacy protection. Elsewhere in the region the picture is mixed. Some countries such as Malaysia and Thailand are in the process of drafting privacy legislation while in other jurisdictions privacy remains in an embryonic or conceptual form. Nonetheless privacy is unquestionably on the map and an increasing number of jurisdictions from India to Japan are placing laws on the statute book that contain privacy provisions.

For us in Hong Kong, the Office of the Privacy Commissioner ("the PCO" established pursuant to the *Personal Data (Privacy) Ordinance*, the "Ordinance") will have been in operation for seven years this December. I would characterise us as having recently moved out of an introductory phase of development and into a phase of consolidation. At least we no longer need to remind the Hong Kong community about their privacy rights or who we are and what we do! Quite the contrary, privacy is very much a daily item in the local media nowadays.

- Relatively few jurisdictions in the region have enacted comprehensive privacy laws or established regulatory systems relating to personal data protection. In fact Hong Kong stands out as one of the very few with a comprehensive piece of legislation that is unqualified by any threshold test in its application.

- As an item on the national agenda of most Asian jurisdictions, privacy occupies a less prominent presence compared with Europe, although there are strong indications that its status is changing driven, as I have said, by a regional approach to privacy issues.

- I would again stress that given the collectivist culture of many Asian economies there has been less of an association between privacy rights and human rights. For example, there are no provisions in some Asian constitutions recognising the right to privacy. The approach therefore towards privacy has tended to be one that seeks to address a particular problem or mischief that has been identified in society e.g. computer crime and spam mail.

5.2 So, the drivers and the approach to dealing with privacy issues in Asia have not necessarily replicated European privacy traditions. That said there can be no doubt that in Asia business interest or concerns around the free flow of data have helped privacy issues to surface. Similarly, technological developments and the rapid diffusion of technology have made Asians acutely aware of the privacy intrusive potential of communications networks.

To that extent nations and economies in the region are no less developed in terms of their use of state of the art technologies in either personal or business communications and transactions. By extension they are no less affected by the issues than their Western counterparts, e.g.

unsolicited E mail, electronic surveillance, unlawful and unauthorised access to personal data in transmission of back-end systems etc.

5.3 The consequence of this has been that Asian and Asia-Pacific economies have quickly come to recognise the critical importance of the protection of personal data as a pre-requisite to securing *E*-trust and *E*-confidence among customers in the B2B and B2C markets. Economic values and the massive benefits to be derived from pan-Asian trade serve as the incentive to put in place a framework of data protection, whether through legislative enactment, self-regulatory mechanisms or a combination of both.

6 Hong Kong's Legacy – A Slice of Europe in Asia

6.1 Given my capacity as one of Asia's privacy commissioners it is incumbent upon me to explain how the PCO regards itself. Naturally our history has played a key role in the development of a privacy regimen that is, I think, generally respected today because of its essentially pragmatic approach to privacy. That pragmatism necessitates a balance be struck between competing interests in our society when formulating policy. I think one of the main drivers in the PCO is that we want to be fair to those that are stakeholders in our policies and, as importantly, we want to be seen to be fair. This characterization is to be distinguished from a heavy-handed interventionist bureaucracy that imposes its will irrespective of the toes it treads upon.

6.2 The Law Reform Commission of Hong Kong began investigating the protection of personal data[2] a decade ago. At that time the then Administration was very much influenced by the British way of doing things. However, it is also true to say that the British had been very much influenced by the European way of doing things by virtue of their membership of the European Union. The legacy of Hong Kong's history has been very influential in developing our privacy regimen and I do not think we have to apologise for that. However, as we have asserted our own identity within the context of the People's Republic of China we have, for want of a better phrase, metamorphosed into something of a hybrid. That is, whilst our origins are acknowledged, our natural alignment today is with China and the Asian community of which we are a part. If the Hong Kong approach is to be defined then I think it is best seen as a synthesis, hopefully of the best elements of the European model and a developing Asian model.

[2] The Law Reform Commission of Hong Kong, *Report on Reform of the Law Relating to the Protection of Personal Data,* August 1994.

6.3 But what does this mean in terms of practical privacy? I think we do have a number of core beliefs that consistently run through our thinking. These may be summarised as follows:

~ we believe in research informing our decision-making and policy formulation and that means finding out and understanding the public sentiments on specific privacy issues;

~ we conduct extensive consultation with interest groups within the community;

~ we believe good policy is policy that works and are very conscious of the need to bear pragmatism in mind at all times;

~ we invariably seek to strike a balance between the privacy rights of the individual, the interests of other groups impacted by our decisions and the public interest; and

~ most importantly, we regard our stakeholders as our partners.

6.4 Although we are privacy enthusiasts and seek to discharge our duties diligently, the PCO is not an advocate of privacy purism. Why? Because such a stance is likely to lead to confrontation and adopting an unduly tough line might take us to a point that we wished we had not traveled. Alienation of segments of our society could well be the likely outcome. We do have a 'stick' but our preference has always been for the carrot, and remains so. We seek by listening to what the community has to say to assist us in determining what is in the best interests of Hong Kong which, as some of our detractors will tell you, is not necessarily the same as doing that which is in the best interests of privacy. So, along the way we have tended to adopt a liberal approach that is flexible yet at one and the same time robust.

6.5 I would like to illustrate by reference to two projects how our approach has reflected our values. Each case portrays the way in which the PCO have sought to achieve a balance between competing interests that has resulted in a solution that is broadly acceptable to the parties, including the PCO.

Case 1: Amendments to the Code of Practice on Consumer Credit Data

6.6 In the earlier part of 2002 approaches were made to the PCO by the Hong Kong Monetary Authority and the financial services sector to assist in formulating a solution to an acute problem in the consumer credit market. The view at the time was that credit providers had insufficient information regarding their customers to be able to make an accurate judgement of their true creditworthiness. A paucity of information regarding the exposure of consumer credit borrowers meant that credit providers were effectively lending blind or half blind. Almost inevitably poor lending decisions were made and, to some extent, these were compounded by evidence of mischief on the part of some borrowers. Throughout 2002, and in fact into this year, the situation degenerated with record numbers of individuals filing for personal bankruptcy fuelled, as some commentators maintained, by amendments to insolvency legislation which had the effect of lessening the traditional stigma attached to bankruptcy.

6.7 The financial impact of these developments became very evident as credit providers began reporting higher and higher charge-off rates peaking at around 11%-12%. This signalled the need to review, with some urgency, the credit management procedures adopted by the financial services sector. It became evident at an early stage in the PCO's investigations that transparency in the marketplace was a significant factor. To correct the situation the financial services sector, and representative bodies associated with it, proposed a relaxation of the provisions of the Code of Practice on Consumer Credit Data ("the Code"), first issued by the PCO in 1998, which restricted the sharing of credit information to so-called 'negative data' (i.e. information exhibiting default in payment).

6.8 As the situation worsened the focus for remedying it switched from credit providers, who were implicated as one cause of the problem, to the PCO. The expectation in the financial sector was that the PCO would play a pivotal role in formulating the solution, and that was to prove the case. However, there was a problem. At multi-party meetings, and in working groups convened to forge a solution, credit providers translated those expectations into a 'wish' list of items of personal data they wanted to collect from individual customers. Without realizing it perhaps the PCO was immersed in the matter of perception management because the financial services sector had already decided the information, so-called 'positive data', that it wished to collect and share through the intermediary of a credit reference agency.

6.9 The PCO was sympathetic to the needs of the financial services sector which is the largest in our economy. To have been otherwise would

have been to disregard the public interest. In this case the public interest argument was predicated on the following points.

- If left unchecked the problems in the consumer credit market would degenerate to crisis proportions with the potential to destabilise the financial markets in Hong Kong.

- Operating in a lending environment characterised by a lack of transparency, and some measure of insincerity on the part of some borrowers, ran contrary to the traditions of prudent banking practice.

- High charge-off rates represent costs to the banks and all consumers would ultimately have to bear those costs.

- The prevailing system permitted a crude categorization that labelled approximately 70% of consumers as 'good credit risk' and 30% as 'poor credit risk.' In effect 'good' borrowers were subsidising 'bad' borrowers. This gave rise to a less-than-equitable situation in which there was no acknowledgement of a 'good' borrower credit status.

Clearly the public interest argument could not be ignored by the PCO but then neither could the personal data privacy interests of the individual.

6.10 There were those in the community who felt that the PCO would be guilty of a betrayal of privacy rights by permitting any relaxation in the provisions of the existing Code. Again, this reflected expectations regarding what some in the community judged was the right thing for the PCO to do, given the circumstances. Understandably, some members of the public did not want to permit the banks to collect additional personal data in the consumer credit market or for them to be able to share that data.

6.11 However, those of this persuasion were outweighed by others in the community. Those others supported the disclosure of additional personal data because they were influenced by banking practices evident in the USA and the UK, which rewarded 'good' borrowers. The suspicion being that the majority of people in this category were of 'good' credits.

6.12 The result of the public consultation exercise (a step mandated by the Ordinance), which yielded 282 responses, indicated that 56% of the submissions made were supportive of the proposals to permit the

collection of additional personal data subject to stringent safeguards being put in place. Individual submissions indicated that the general public were aware that there was a trade off to be derived from credit providers having access to additional items of positive credit data, namely:

- consumers with good credit positions would be able to benefit from the proposal since they would be more likely to obtain better credit terms;

- a positive credit rating would be shared with other lenders in the scheme; and

- a good credit rating could be regarded as a personal asset.

6.13 In this project the PCO had to balance at least three sets of expectations. In the first instance, a broad range of credit providers in the consumer credit market shared the view that the disclosure and collection of further items of positive credit data would address the problems experienced by lenders. It was expected that the PCO would respond in an appropriate way to those needs out of a duty to serve the public interest.

In contrast, data subjects in the community were divided. Of those who made individual submissions 50% were in support of the proposals permitting credit providers to collect and share additional items of personal data. However, 41% were opposed to the proposal and the balance gave no indication one way or another but many of whom offered suggestions (some very valuable and sensible ones) which they expected the PCO to adopt.

6.14 In terms of managing public expectations, the realities coming out of the exercise could well have done the frustration of at least one set of expectations in the community. Certainly the submissions that were opposed to the amendments made it very clear that the PCO would be failing in its avowed mission if it were to permit the collection of *any* additional data by credit providers. Taken one step further accusations were made that any such proposal would be tantamount to serving the interests of big business. Furthermore, in using the public interest argument in the consultation document and media interviews, the PCO were held, by some, of being more committed to a nebulous concept relating to the 'best interests' of all citizens and subordinating personal data privacy rights of the individual. I personally do not agree with this interpretation but I can understand it.

6:15 It is easy to speculate that those submissions protesting the relaxation in Code provisions could have been dominated by individuals who might have been in financial difficulties with credit cards or personal loans. However, that is pure speculation, and, even if it were true, would not necessarily invalidate those individuals' objections in the context of data privacy in its purer form. The lesson for the regulator is, I believe, that we need, at a minimum, to be cognisant of the consequences of what we do in terms of policy. The dilemma is that in trying to satisfy one set of expectations we may effectively alienate a contrary set of expectations. In the end we need to ask ourselves whether, in projects of this nature, it is practical to move beyond a solution that is optimal for one section of the community and sub-optimal for another. Is this the best we can realistically hope to achieve? If so, then people such as myself will have to live with the fact that in situations where there are competing interests or expectations we are condemned to a role in which a win/ win solution may not be an achievable objective.

Case 2: The (proposed) Code of Practice on Monitoring and Personal Data Privacy at Work

6.16 In the first case, amendments to the Code of Practice on Consumer Credit Data, the response by the PCO was to the needs of the financial services sector i.e. the solution was industry-specific. The second case I would like to review is both very different in substance and relates to industry, more specifically employers, in general. The proposed Code of Practice on Monitoring and Personal Data Privacy at Work ("the Code") was drafted in 2002 as a policy response to the following factors.

- In 1999 the Sub-committee on Privacy of the Hong Kong Law Reform Commission ("the LRC") issued a consultation paper titled: *Civil Liability for Invasion of Privacy*. In the paper the LRC made the following recommendation that:

  "The Privacy Commissioner for Personal Data should give consideration to issuing a code of practice on all forms of surveillance in the workplace for the practical guidance of employers, employees and the general public."

- A survey conducted among data users in 2000 indicated that 64% of employers in Hong Kong had installed at least one of five types of surveillance[3]. One in every three employers surveyed had two or more surveillance systems in the workplace. What the

[3] The surveillance facilities investigated included: CCTV/video, telephone, E mail web browsing and PC usage.

survey clearly revealed was that workplace surveillance was pervasive. More employees in Hong Kong, as elsewhere, are being monitored by more forms of surveillance device than ever before. It is only reasonable to expect that trend to continue and for it to manifest itself in small and medium sized enterprises.

- ❒ However, rather more disturbingly, from an employees perspective, only 18% of employers surveyed had a written policy on workplace surveillance. In short, requirements pertaining to notification of the purpose of workplace surveillance were, at best, less-than-transparent and, at worst, had probably been ignored altogether.

- ❒ It was also evident from a data subjects survey conducted in the same year that employees did have some expectation of privacy in the workplace. For example, they did have distinct views about the intrusiveness of particular workplace surveillance practices:

  - ~ interception of private telephone conversation;

  - ~ viewing of contents of employees E mail sent or received on a company supplied computer; and

  - ~ logging of all calls made by an employee during working hours.

6.17 It is evident that employees do have some expectation of privacy in the workplace and that they do not expect to forfeit their privacy rights as a consequent of employment. This view is at variance with the position adopted by some employers, gratefully not all employers.

6.18 From our discussions with employers, and the submissions made in response to a public consultation exercise, it is very clear that data users hold to a different view. One position taken by employers is that the privacy rights of the individual are diminished upon entering the workplace. That is, managerial prerogative dictates the absolute right of the employer to manage the resources and assets of the business and that includes communications equipment whose primary purpose is to facilitate work. Where an employer exercises discretion and permits reasonable use of communications equipment for personal purposes the employer reserves the right to ensure that the employee does not abuse the facility or use it for improper purposes. The argument here is that it would amount to negligent stewardship if the employer did not take

appropriate measures to monitor the use of communications equipment. Justification for so doing varies from measuring productivity, monitoring customer service delivery and vicarious liability of the employer for any wrongdoing committed by an employee.

6.19 These respective positions are indicative of a disjuncture between employees and employers and represent markedly different expectations. Ultimately, it comes down to a relatively simple question which the community has to answer: Is an expectation of privacy in the workplace, beyond the very obvious, a legal entitlement of the employee or is it a matter to be determined at the discretion of the employer?

6.20 Satisfying both sets of expectations is likely to be difficult. This is reflected in the deliberation we are currently giving to issuing either a code or guidelines. Under our law, an infringement of a code issued by the PCO would give rise to a 'rebuttable presumption of contravention' of the Ordinance. In contrast, guidelines would not carry an equivalent legal status and amount to the PCO's recommended or best practices. Unsurprisingly, some quarters of the community have called for greater restraint by the PCO and the issuing of guidelines which are perceived to be more flexible and less onerous for employers to comply with. Employers have supported this position with the following arguments:

- There is, at least in Hong Kong, no evidence of abuse on the part of employers in their workplace monitoring practices.

- Against that background, there is no justification to introduce a code, which would become a further imposition and add costs to their operations.

- 'Legislating' matters pertaining to employee relations is an inappropriate approach in an employment context characterized by mutual trust and respect between employers and employees.

6.21 It would not be easy to find common ground that would satisfy the legitimate interests of employers and the personal data privacy interests of employees. Of course, the ultimate responsibility resides with the employer in terms of complying with the requirements of the Ordinance. However, if we are to regard the employer as a 'stakeholder' (which is obviously the case) and therefore our 'partner', it is incumbent upon the PCO to make that compliance goal easier, though by no means easy, to attain. It follows from there that we need to work with both employer and employee to find the right solution which would, to the extent that is practicable, strike a balance between the two alternative sets of interests

that are common to industry in general: those of the employer and those of the employee.

6:22 At present we are undertaking a cross-jurisdictional analysis to better understand approaches to workplace surveillance in other privacy regimens. If we dismiss 'doing nothing' as a possibility there are essentially three options open to us.

- Issue a comprehensive Code of Practice on Monitoring and Personal Data Privacy at Work. Under our Ordinance this would be of a different legal status to the UK's Employment Practices Data Protection Code [Part 3 ~ Monitoring at Work]. A code would be the most robust form of protection of employees privacy rights – short of dedicated legislation - but we are also fully aware that we should neither ignore the expectations of employers nor should we antagonise their interests.

- Alternatively we could adopt a more conciliatory 'hybrid' approach. Given that there is 'no contest' on the principle of transparency the PCO could address this aspect of workplace surveillance and incorporate it into the provisions of the Code of Practice on Human Resource Management. The remainder of our proposals could be published as guidelines.

- Thirdly, we could issue a comprehensive set of guidelines which would amount to management best practices. These could be an integral part of a two step strategy. The guidelines that would be issued in the initial part of the strategy would aim to encourage employers to formulate in-house policies and adopt practices that were compliant with the provisions of the Ordinance. After a period of say two or three years the PCO would revisit the situation, conduct a survey of practices and on the basis of the findings decide whether guidelines were effective in producing the desired outcome. If that were not found to be the case then the fallback strategy would involve the second step which would be to issue a comprehensive code of practice under Section 12 of our Ordinance.

6.23 In all probability a different option would be selected as the better option by the respective camps. Therein lies the dilemma because one set of expectations demand a 'hands-off' solution that affords employers considerable flexibility. On the other hand, the expectations of employees would most likely translate into a more robust 'hands-on' solution that afforded better protection for the individual. At this point, I can only advise that work is continuing.

7 Current Asian Privacy Initiatives

Asia-Pacific Economic Cooperation (APEC) ~~ Electronic Commerce Steering Group (ECSG)

7.1 Surveys of consumers in the Asia Pacific region have consistently shown their reluctance to engage in *E*-transactions and naturally this has impeded development of this trading mode which possesses vast potentials. In seeking to address consumer anxieties, APEC has decided to undertake initiatives that would have the effect of establishing consumer trust and confidence and in the process also promoting cross border trade within the region. It was also acknowledged that the true potential of electronic commerce could not be realised without government and business co-operation.

7.2 In 1998 the APEC ministers endorsed a ***Blueprint for Action on Electronic Commerce.*** In a Leaders' Declaration, the ministers recognized *"the enormous potential of electronic commerce to expand business opportunities, reduce costs, increase efficiency, improve quality of life and facilitate the greater participation of small business in global commerce".* It was agreed that *"Government and business should co-operate 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, authentication and consumer protection."* It was further agreed that the role of governments include *"providing a favourable environment, including legal and regulatory aspects, which is predictable, transparent and consistent"* and developing *"domestic frameworks which are compatible with evolving international norms and practices".* This statement of intent sets out clearly the mandate, the priorities and the incentive to address data privacy issues in the region's efforts to exploit the vast potentials in electronic commerce.

In February 1999, the Electronic Commerce Steering Group (ECSG) was established to take the initiative forward. All 21 APEC economies are represented on the Steering Group[4]. The primary purpose of this forum is to ensure the continued co-ordination of APEC E-commerce activities.

[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.

The ECSG organized a privacy workshop at Mexico City in February 2002 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 economy for APEC with workshops and meetings held in Chiang Rai (February 2003) and Phuket (August 2003). Following Chiang Rai, a Data Privacy Sub-Group[5] was established with the mandate to develop a set of privacy principles and implementation mechanisms.

APEC Privacy Principles

7.3 APEC's privacy initiative 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 economies. One of the principal aims of the initiative is to establish trust and confidence in *E*-business thereby modifying consumers' perceptions towards online transactions.

7.4 The diversity and richness of Asian cultures are reflected in the value attached to privacy and this has resulted in variations afforded to their citizens. 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 closer 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.

7.5 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. 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.

7.6 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 reflective the characteristics and needs of APEC member economies. 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 progressed the picture that has emerged is that member economies, whilst acknowledging the contributions from the European evolution of the concept of data privacy, would prefer to address the issues from a regional perspective. My view is that this mentality lends a freshness to the initiative, which should be given the opportunity to demonstrate its worth, and a consensus outcome is more likely to be achieved and therefore acceptable to the economies.

7.7 My APEC colleagues and I have already worked through several versions of the draft privacy principles and there will be more versions before the work is done[6]. When these principles fundamental to a privacy regime are settled, we can then move on to implementation mechanism and international cooperation which will ground the framework for transborder data flow. There are many important issues to be discussed and resolved, not least, the Australian proposal on ' self-certification' as a basis for mutual recognition between data protection jurisdictions. I remain confident that at the end of the day the forum will have produced a very credible document that upholds the traditions of personal data privacy protection whilst at the same time reinvigorating them.

7.8 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 privacy guidelines. I shall briefly discuss the APT initiative in a moment. Evidently, there is a need to ensure that there is no inconsistency in the output of these separate endeavours. One suggestion has been to incorporate aspects of the APT Guidelines into the APEC Privacy Framework, 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 Framework as offering core regulatory guidelines at the macro level. In contrast the APT Guidelines, at least in their first draft, address day-to-day information management and provide a model code

[6] Privacy Principles currently being discussed relate to: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability.

at the operational level, which takes account of regional diversities. Hopefully, the two instruments will be compatible and work in favour of the communal interests of all member economies.

Asia Pacific Telecommunity (APT)

7.9 In response to an inter-governmental agreement the Asia Pacific Telecommunity[7] ("the APT") was established in 1979 as a regional telecommunications organization. The APT operates 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 countries. The survey findings were reported at the 22nd APT Study Groups 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[8].

7.10 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 APT initiative seeks to give recognition to 'Asian' diversities in terms of cultural, social and economic differences, greater reliance on governmental role and a more communal approach towards data privacy. There are three basic purports in the current draft, namely, to guarantee

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

[8] The project is led by the Korean Information Security Agency (KISA), which produced the first draft of the APT Guidelines.

the right to self determination over personal information as an aspect of human right, to secure the confidence of users of e-commerce and other electronic services, and to facilitate free transborder flows of personal information in the region. 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 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.

Asia Privacy Forum

7.11 Data privacy as a regulatory concept has been accorded lesser attention in Asia than in the West due in part to different cultural background which emphasizes harmony within communities over individualism. However, advances in information technology (IT) and the 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 users. It is probably true to say that nations and economies in Asia 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, e.g. Spam and unsolicited email, surveillance, etc.

7.12 Whilst 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. Recognizing 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,
- to better understand the specific issues that confront individual jurisdictions,
- to identify commonalities in those issues, and
- to the extent possible, to coordinate efforts to identify solutions to matters of common concern.

7.13 Closer regional co-operation has paved the way for the emergence of the Asia Privacy Forum[9] ("the APF"). An informal meeting was hosted by the 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. The forum seeks to promote data privacy protection in the Asian Region and in so doing give due recognition to regional similarities and diversities in the context of cultural, social, governmental and economic realities prevailing in individual jurisdictions. Participation at the forum operates on what may loosely be described as 'agency to agency' basis and participants include data protection authorities, officials from government departments and public authorities, NGOs as well as privacy advocates. Such diverse participation enables the forum to maintain informal and flexible operational characteristics without the constraints usually associated with national representations.

7.14 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 regimen.

7.15 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[10]. It is intended that the forum will function at the operational or working level with the aim to identify and adopt solutions to privacy issues common to the members. Working groups are in the process of being established and they will spearhead the early work of the APF[11].

---

[9] 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 (InfoComm 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).

[10] The main issues of common concern are: Unsolicited E-mail and spamming, employment privacy, E government/ E business, identity theft, biometric data, misuse of personal data by businesses and regulatory and enforcement difficulties.

[11] The proposed working groups are: Asia Privacy Guidelines, Spam/Email, Public Awareness of Personal Data Protection and Data Protection Inventory.

8 Developments in Regional Jurisdictions

8.1 The Asia-Pacific nations and economies participating in the 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.

8.2 In 2002, the APT convened a Study Group to tackle info-communication issues faced by the region. A Study Question, "Personal Data Protection in the Asia-Pacific Region", was taken up and the Korea Information Security Agency (KISA) was entrusted by the APT Study Group to undertake a comprehensive survey of the personal data protection frameworks found in APT member countries. KISA's report was released in August 2002. The report provides a broad picture of the current status of privacy protection in the region. There have also been further developments in individual jurisdictions since the publication of the report, and I have added to my comments below information that has come to light in the course of our liaison with neighbouring economies.

Legal Framework

8.3 Several member jurisdictions within APT have operationalised their data privacy regimes for some years and 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. (Obviously, privacy developments in jurisdictions such as Australia and New Zealand are familiar to this audience. There is no need for me to comment further for the simple reason that there are colleagues from these two countries in the audience who are eminently better qualified than I to undertake that task.)

8.4 Others in the region that do not have specific privacy legislation do, nonetheless, recognize the need to address the issue in their general legal framework and have introduced 'privacy' provisions in their sectoral regulations. For example, India regulates wiretapping through a sector specific law on telegraphy, and Bhutan and Lao PDR impose varying degrees of responsibilities on Internet service providers. 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. Others, who have established specific privacy legislation, have sought to strengthen or give practical effect to statutory provisions by the issuance of guidelines or codes of practice to assist industry sectors to be compliant. Australia, Hong Kong, Korea and New Zealand provide good examples of this approach.

8.5 Japan, which, until quite recently, did not have privacy legislation specifically targeting the private sector, has also made extensive use of self-regulatory guidelines to promote compliance. In Japan, the proposal to extend personal information protection to the private sector was discussed (at the community level and in the Diet) for many years. A government bill dealing with private sector regulation was introduced into the Diet, generating considerable discussion and controversy, and was subsequently withdrawn in 2002. Earlier this year (January 2003) it was re-introduced into the Diet with amendments responding to criticisms and offering concessions to media interests. However, the concessions made were met with critical comments by privacy advocates. Nonetheless, the bill passed the Lower House in May this year, went to the Upper House for further deliberation, received an affirmative vote later in the same month and was signed into law.

8.6 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.

8.7 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 globalized world. It may be fortuitous that that phenomenon has resulted in the realization of the need to harness that value by way of establishing a framework of personal data protection.

Personal Data Protection Principles

8.8 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

8.9 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 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 amongst those who provide protection to data subjects not resident in their jurisdictions.

Personal Data Protection Authority

8.10 Australia, Hong Kong, Japan, South Korea and New Zealand have all established dedicated civil authorities to oversee compliance with legislation on personal data protection. Necessarily, their constitutional status and operational methodology differ, depending on local conditions and the background to their respective privacy regime being established. Hong Kong, for example, has created the PCO as an independent statutory body (a corporation sole in terms of our law). Others may have closer ties to local government (which is not necessarily a bad thing, provided the authority is able to regulate and discharges its function in an independent manner).

8.11 From this very brief summary, it should be apparent that the same few jurisdictions were mentioned as examples of ongoing regulatory privacy systems. To an extent, this represents the current status of development in the region but it does <u>not</u> represent a dearth of interest or commitment on the part of those that have not been mentioned. There are issues common to all jurisdictions. SPAM and unsolicited emails (with implications on system security) are obvious examples. Their common occurrence is matched by a common inability (so far) to come up with

solutions. Some jurisdictions attempt to tackle the nuisance via legislation (Korea, for example, has enacted legislation, and Hong Kong is thinking about it) but how successful that legislation will be as a 'final' solution remains to be seen. No one, I suspect, would be prepared to underestimate the determination and ingenuity of the perpetrators. This, and other issues, ensures the cooperation of jurisdictions to identify and adopt a common stance.

8.12 Social and economic developments are important considerations for many countries in the Asia-Pacific region, and, if I may say, rightly so. From that standpoint, the perceived economic benefits inherent in electronic commerce provide an incentive to establish a data protection framework. From the APT report released by KISA, it is clear that countries in the region recognize the pre-requisite to promoting E business is to establish a data protection regime. That regime must also be one that represents regional consensus, which, in turn, ensures cross-jurisdictional cooperation in trans border flow of personal data across national boundaries. Fulfillment of that pre-requisite is viewed as instrumental to the release of economic benefits from electronic commerce.

8.13 There is an apparent chorus amongst jurisdictions, which are at varying stages of 'privacy' development, calling upon the more developed to provide technical support and impart knowledge through forums, conferences and workshops, and, in some cases, financial assistance. A case is being made out for the establishment of a cooperative body which can reflect views that take account of local conditions among the regional jurisdictions. Progressively, the concept of promoting regional privacy guidelines and model regulatory structures with an emphasis on cross-border cooperation is being viewed with favour. Once again, prospects of regional prosperity will provide the incentive to move this concept forward.

Raymond Tang
Privacy Commissioner for Personal Data
Hong Kong SAR

12 September 2003