Privacy Laws and Business
16th Annual International Conference

Transforming Risk Assessment into Everyday Compliance with Data Protection Law

7-9 July 2003 – St John's College, Cambridge, U.K.

Session - International Data Protection Law

7th July, 2003

Partners in Privacy – Working Towards a Privacy Aware Society in Hong Kong

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 Over the past decade or so there has been, in many societies, a burgeoning of interest in personal data privacy, privacy in the more generic sense and privacy-related issues. This has certainly been the case in Hong Kong and yet, in a Chinese context, this appears to be a little surprising. This is because in Chinese society the concept of privacy in a modern sense is relatively new. In Chinese vocabulary, the word for "privacy" connotes the notion of secrecy or an aspect of the person that the individual would prefer to conceal. As a result, privacy relating to personal data, which is the principal concern of the Office of the Privacy Commissioner for Personal Data ("the PCO"), was a relatively novel concept. However, this situation has changed significantly over the past six years, which coincides with the date of the PCO becoming operational.

1.2 Given the cultural dimension to privacy in a Chinese society our experience in Hong Kong offers a case study that may hold lessons for those seeking to both diffuse the notion of privacy and popularise it. In my opinion I think we have been able, over the period we have been in existence, to lay reasonable claim to having achieved two important goals. Firstly, we have managed to move from a state of low, or no, awareness in the community regarding privacy rights to one in which those rights are understood. I do not claim that the inhabitants of Hong Kong could recite those rights at will but the evidence is that they recognise that they have rights and that those rights are protected by the provisions of the Personal Data (Privacy) Ordinance ("the Ordinance") which my office regulates. Secondly, and, more significantly, the community value the rights conferred upon them. The evidence to support those claims will be presented in due course in this paper. The 'measures' we have suggest that our operations and communication strategies have been on target during a period that I would describe as the PCO's pioneering phase. Having made these gains we want to build upon them in what, I think, could be regarded as the next phase, a period of consolidation.

1.3 I would like therefore in this paper to share our collective experience with you and offer some insights of where we have come from, where we are now and the immediate outlook. In so doing the intention is not to convey the sense that the PCO has divined some sort of privacy blueprint. Rather, it is an approach that has suited the Hong Kong context. I should perhaps add in passing that Hong Kong has a relatively 'mature' privacy regimen when compared with most other Asian jurisdictions and we hope that will enable us to be of assistance to those who may find our approach worthy of scrutiny.

1.4 From the research we have conducted over successive years it is evident that protection of personal data is seen as an essential right and important area of social policy; and this is encouraging. In 1994 when the idea of a privacy commissioner's office was being debated the community seemed a little indifferent to the notion of privacy and, in some instances, confused by it. At that time a primary stimulus for establishing the PCO came from the business sector which was anxious to conform with the OECD's Data Protection Guidelines that addressed the matter of trans-border data flows. However, from this early expression of interest the concept of privacy, and more specifically personal data privacy, has become more diffused. It is that aspect of our work, that might conveniently be labeled the 'diffusion and adoption of privacy' that will be the focus of this paper. In the course of developing my arguments I hope, what will become apparent, is the way in which we have tried to involve the community, and sub-sets of it, as partners in privacy. I am of the view that we would not have enjoyed the measure of success that we have, had we had not mobilised the support of the community and joint-ventured with them in the development of privacy policy. An alternative would have been to venture out on our own. We elected not to do this because we regarded community support as an essential part of our collective endeavours to create awareness and, quite frankly, because we could not have achieved what we have with the limited resources available to us.

1.5 The joint focus of our work on a day-to-day basis continues to be on developing community awareness and encouraging voluntary compliance. However, beyond these perennial objectives we have set ourselves a superordinate, and very important, social goal. That social goal is the universal respect by all citizens of another person's personal data privacy. The ideal state would be one in which we constructed a culture conducive to extending that respect to the wider remit of privacy per se i.e. beyond the boundaries of legal requirements and limitations. Ultimately, the desire would be to make privacy something that is inherent in the individual and a collective community value: an essential part of the composition and upbringing of future generations as complete members of a modern society. The next five years will set the tone for achieving this goal.

1.6 At this early juncture it is perhaps worth recording that not all quarters of our society are strong supporters of our work and we have our critics. This has accentuated the need for the PCO to balance the competing interests evident in our community. Reference will be made later on to our thinking regarding the way in which we have managed to accommodate competing interests and, in so doing, avoid alienating sections of society. This is

critical in terms of relationship building, influencing opinion and strengthening the partnership I have alluded to. Of course, we have not managed to please all of the people all of the time but we strive at least to understand their needs and address them.

Before going into more detail regarding the approach, and modus operandi of the PCO, it is desirable to at least attempt a definition of the term privacy and, in particular, personal data privacy.

2 Privacy and Personal Data Privacy

2.1 It was the French philosopher and writer Voltaire who once said, "Define your terms and we shall talk." This is easier said than done insofar as the generic concept of privacy is concerned. In spite of the significant growth in interest expressed in privacy by academics, lawyers, IT professionals and members of the global privacy community, an all encompassing definition that has broad based approval seems as elusive as ever. This is possibly the result of privacy being a deeply personal concept lacking in readily definable parameters. It is also something of a moving target. That is, privacy is constantly being redefined by the application of new technologies and current events. Even then, this takes no account of the expediency exercised by the political authority of the day.

2.2 At the PCO we have largely avoided tackling this difficulty because we are primarily concerned with information privacy or what in Hong Kong is termed personal data privacy. In essence the provisions of the Ordinance regulate the activities of data users i.e. collectors of personal data, in terms of their use of the personal data of the individual i.e. the data subject. In so doing the law endows the individual with personal data privacy rights derived from six Data Protection Principles ("the DPP") that give legitimacy to those rights [please refer to Appendix I]. The DPP are modeled on the substance of the OECD principles and will be reviewed in a little more detail later on.

2.3 Personal Data are those identifiable pieces of information such as: name, address, age, identity card number, salary, marital status, phone number, E mail address, personal image, financial status, opinions held by the data user of an individual etc. By this definition personal data assumes a similarity with the term information data used in other jurisdictions but is not identical with it. More specifically personal data are defined in the Ordinance as:

" relating directly or indirectly to a living individual; from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and in a form in which access to, or processing of, the data is practicable ..."

What this means is that there must be a tangible record of personal data whether that be a database containing details of customers, or a CCTV tape held by an employer that contains the image of employees. It is also worth mentioning that, in an Appeals Court ruling, personal data is only regarded as personal data if the data user *compiles* the data with the intention of identifying a particular individual.

2.4 This definition has worked well in practice and has allowed the Hong Kong regulator to adopt a more pragmatic approach towards data privacy. The Ordinance is a comprehensive piece of legislation that runs to some seventy sections plus schedules. The concept of personal data privacy is captured and embodied in a set of data protection principles and flexible statutory provisions which allow the Commissioner to deal with 99% of complaint cases that are investigated. However, one downside of the Ordinance is that it is virtually impossible to communicate to a mass audience. In seeking to popularise it we have had to choose our messages carefully and communicate them with clarity and consistency. Only by so doing would we have been able to raise levels of awareness which, as I say, were negligible when we began operations. Largely speaking, with the exception of expert or special interest audiences, we have maintained this stance in our communications strategy because there is a distinct appeal in simplicity. Regrettably, simplicity is not a term that could be used to characterise the provisions of the Ordinance.

2.5 Although clarity of message has been key to creating awareness it has also fuelled the desire in the community for ' more of the same.' At this point that need has largely gone unanswered because those aspects of privacy that members of the community are interested in seeing addressed by the PCO e.g. media intrusiveness, are not covered by the provisions of the Ordinance. To that extent there is something of a ' frustrated demand' in the community that will, at some stage in the future, have to be tackled. Clearly, it is necessary to address the shifting needs of the community but, more importantly, it is necessary to mange the perceptions of the community and align them with the realities of the constraints under which the PCO operates. I will make reference to perception management in due course because experience has brought me to the conclusion that this is an essential part of our communications strategy. If community expectations are left unchecked then there is the very real prospect of a divergence

between the needs we endeavour to satisfy and the needs expressed by the ‘customer.’

3 Local Drivers Leading to the Establishment of the PCO

3.1 The establishment of the PCO in December 1996 was a response to four main drivers.

- The position and significance accorded to data/information privacy by the European Union and a succession of directives from it regarding the norms to be applied to such data.

- Appeals from Hong Kong’s business community to address the issues posed by trans-border data flows and the need to avoid any constraints upon trade.

- A 1994 Law Reform Commission Report recommending the reform of laws pertaining to the protection of personal data privacy and the creation of the Office of the Commissioner for Personal Data.

- Obligations imposed upon Hong Kong as a signatory to international covenants e.g. the International Covenant on Civil and Political Rights and the Hong Kong Bill of Rights.

These events coalesced at around the same time reinforcing the recommendation put forward by the Law Reform Commission. In addition, the time seemed opportune because of changes in the technological, social and economic environments. I will briefly overview the influence of each of these factors.

3.2 Technological Factors

Hong Kong exemplifies a consumer marketplace in which new technology finds a ready and eager consumer market. For example, the mobile phone market has reached saturation levels yet approximately half of all mobile phone owners change to an upgraded model each year. Another indicator is the market for pre-recorded VCD’s. This format has declined drastically largely because of the popularity of the DVD. However, perhaps the greatest passion for technology has come with the PC which is regarded as just another consumer durable. Something like 50% of all domestic households have at least one PC and the vast majority have access to the Internet.

However, with the growth in ownership of PC's and Internet usage there has been a concomitant development. Successive surveys, and our own research, indicate that there are low levels of trust and confidence in the integrity of personal data both in transmission and in back-end systems. As a result the predicted boom in B2C E-Business just has not materialized. For example, a recent survey conducted in May of this year revealed the following findings.

- 83% of general Internet users feel that limited personal data protection restrains Hong Kong's E-business development.

- 86% of survey respondents felt that E-privacy, or security problems, would dissuade them from making payments online[1].

Our own public survey also revealed that consumers in Hong Kong placed privacy protection ahead of quality of service, range of choice and pricing when evaluating the importance of factors that would affect a decision to purchase online. These findings provide a good illustration of a commonly held perception, rightly or wrongly, that there is greater risk in buying online with a credit card than buying in the physical marketplace also using a credit card. This perception continues to prevail and in so doing acts as an obstacle to E-business thereby frustrating its potential.

Such anxieties explain why, in Hong Kong, consumer expenditure online is only in the region of 1%-2% of total consumer expenditure. The infrastructure is there, and citizens have a high level of familiarity with it, yet privacy concerns remain a major stumbling block to online purchasing.

It is reasonable to conclude that technological convergence, digital advances, miniaturization, the advent of the information age and the E-Business economy have, on the one hand, brought considerable benefits in terms of product pricing and convenience. On the other hand it is equally clear that the community in Hong Kong sees significant privacy risks in terms of the management of personal data by online data users. Of greater concern is the fact that this perception in the community has remained unchanged in spite of the best efforts of E-business to reassure consumers.

As the PCO operates on the belief that what is unlawful offline is unlawful online, there is a duty on the part of the PCO to ensure online compliance

[1] The findings are taken from a study conducted in May 2003 by the IT Practice Group of Stevenson, Wong and Company http://www.sw-hk.com

with the Ordinance. This is a task to which we have devoted considerable time and resources.

3.3 Social Factors

Over the past few years there has been a great deal of interest shown in privacy and privacy-related issues in Hong Kong. The debate has transcended all levels of society from the government, to professional associations, to the man in the street. Interest in privacy is reflected in the growth of privacy groups and the exposure given to privacy by the media where the subject has become a daily news item. Not only does privacy have its own political advocates in our Legislative Council but it is also now a constituent element of university law studies.

I like to think that this level of interest has, in good measure, been stimulated by the work of the PCO. What is not in doubt is that social change has had a profound and sustained impact upon the community which in turn has impacted their perceptions and attitudes towards privacy. Earlier debate has moved on from being of primary interest to privacy advocates, to becoming a phenomenon that virtually everybody has come to regard as a fundamental right they wish to protect and exercise. The heightened profile of the public debate on privacy has produced four main results.

- First of all there has been an increase in the value assigned by the individual to *who* uses their personal data and for *what* purpose(s).

- Secondly, there is now a firmly established desire on the part of individuals to exercise *control* over their personal data.

- Thirdly, the individual expects data users to inform them of any *change of use* of their personal data which should be conditional upon the *consent* of the data subject.

- Finally, and the most rewarding thing, is that privacy has established itself as *a human right*; a right that is recognised under the Basic Law that governs the Hong Kong Special Administrative Region of China.

3.4 Economic Factors

The move towards a global economy has largely eroded the classic protectionist mentality of trading nations. The protectionist creed had, for

decades, been used to defend domestic industries, or entire economic sectors from the competition of imports. As a consequence, markets became inefficient, prices were held at an artificially high level and in general the consumer suffered as a consequence. However, this is a far cry from the liberalisation of trade and dismantling of tariff barriers that has occurred over the past two decades. Bi-lateral trade has given way to multi-lateral trade due mainly to the impetus of powerful trading blocs such as the European Union and ASEAN. More recently, this trend has been taken to its logical conclusion, the globalisation of trade, characterised by a vision of one world, one market.

The importance of this global economic development is not lost upon those in the privacy community. The most serious concern is in terms of the capacity of data users to transfer vast quantities of personal data across international borders. Without the appropriate controls in place this is a worrying development because the personal data of millions of individuals can be used as the raw data for profiling and use in marketing programmes that assume global proportions.

The combined effect of these factors has been to bring into sharp focus the fact that the protection of privacy has now become a truly international activity. The issuing of a landmark set of Data Protection Guidelines by the OECD in 1980 was implicit recognition of that. This initiative has, of course, been further developed by the European Union which, in 1995, issued a directive on the protection of individuals with regard to the processing of personal data and the free movement of such data. The purpose of issuing the directive was to ensure that, unless there were adequate protection of personal data in countries outside the European Union, trans-border transfer of personal data could be interfered with, if not suspended, between EU member states and third party countries. Given that Hong Kong's economic success is in large part due to its export-driven competitiveness it became apparent to the Administration that the economy could not afford to be competitively disadvantaged by not having a legal data protection regimen that met the requirements of the EU directive.

4 Hong Kong's Approach to the Protection of Personal Data Privacy

4.1 It was against the background of these developments that the Government of the HKSAR decided it was appropriate to commit to statutory protection of personal data privacy. The rationale for this decision was based upon four main arguments.

- ❒ Prior to the enactment of the PD(P)O it was felt that the OECD's data protection guidelines were not comprehensively addressed by any existing legislation in Hong Kong.

- ❒ The alternative to the statutory regulation of personal data privacy was self-regulation. However, it was felt that this would result in a piecemeal 'solution' and would fail to offer either adequate or comprehensive protection of privacy rights at a time when there was some evidence of increased invasiveness of privacy.

- ❒ The international transfer of personal data, that is frequently a prerequisite of international trade, necessitated reciprocal measures if the free flow of data to and from Hong Kong were to be guaranteed.

- ❒ International covenants and statutory obligations required the government to both advance and protect privacy as a human right.

4.2 In 1994 the LRC reviewed the status of privacy in other jurisdictions. This review indicated that there were three macro approaches towards institutionalising the protection of privacy.

Option 1

- ❒ Institute a statutory framework and regulatory body funded by the State.

Option 2

- ❒ Create a statutory tort of invasion of privacy to permit civil proceedings[2].

Option 3

- ❒ Rely upon self-regulation e.g. voluntary Codes of Conduct and professional/industry watchdogs.

[2] In a consultation paper issued by the LRC in 1999 two recommendations were made. Firstly, that there should be a statutory tort of invasion of privacy against *"…any person who intentionally or recklessly intrudes, physically or otherwise, upon the seclusion and solitude of another or into his private affairs or concerns."* The second recommendation proposed that *"…any person who gives publicity to a matter concerning the private life of another should be liable for a statutory tort of invasion of privacy provided that the disclosure in extent and context is of a kind that would be seriously offensive and objectionable to a reasonable person of ordinary sensibilities and he knows, or ought to know, that such disclosure is seriously offensive and objectionable to such a person."*

The LRC took the view that it was in Hong Kong's best interests that internationally agreed data protection guidelines be given statutory force both in the public and private sectors. Prior to the drafting of this report, independently commissioned research surveyed public attitudes towards privacy. The findings of that survey indicated that there was broad based support in the community for the statutory protection of privacy.

5 The Personal Data (Privacy) Ordinance

5.1 In response to the LRC's final report the then Hong Kong Government set to work on drafting the Ordinance, the provisions of which were to be regulated by an independent statutory body, namely the Office of the Privacy Commissioner for Personal Data. In effect the PCO is a manifestation of Option 1 although it embraces elements of Options 2 and 3. The statutory framework afforded by the Ordinance ensures the independence of the PCO as a regulatory body, permits civil redress for any contravention of the provisions of the Ordinance, and empowers the Commissioner to promote self-regulation through issuing Codes of Conduct. To date the PCO has issued three such codes: the Code of Practice on the Identity Card Number and other Personal Identifiers; the Code of Practice on Consumer Credit Data; and the Code of Practice on Human Resource Management. A proposed fourth code, the Code of Practice on Employee Monitoring and Personal Data Privacy at Work, is currently under consideration after a public consultation exercise.

5.2 The Ordinance came into effect in December 1996 and established the PCO to monitor, supervise and promote compliance with the Ordinance. The essential scope of the Ordinance can be summarised as follows:

- ❒ application directly, or indirectly, to a living individual;
- ❒ universal coverage extending to the private, public sector and any individual that collects personal data; and
- ❒ application to automatic and manual data formats that result in the creation of a record.

Under the Ordinance the Commissioner is empowered to investigate suspected breaches and, where appropriate, enforce compliance by issuing an enforcement notice. As a result, a primary function of the PCO is to answer enquiries (16,352 of which were received in the year-end to March

2003) and investigate complaint cases (906 of which were received in the year-end to March 2003).

5.3 The functions and powers of the Commissioner as articulated in the Ordinance cover the following main areas.

- Monitoring compliance with the provisions of the Ordinance by data users. Complaints that pass an initial prima facie screening process are investigated by staff of the Operations Department. As a matter of principle the PCO much prefers to act as a mediator between the complainant and the party complained against rather than resorting to the big stick, although we are not averse to so doing when warranted. To date our experience indicates that approximately 70% of complaints are filed against private sector data users, notably banks, real estate agents, telecommunications providers and life insurance companies. A further 20% are filed against government departments and agencies, and 10% are filed against individuals.

- The approval and issue of codes of practice, that offer practical guidance for compliance with the provisions of the Ordinance, which require the PCO to undertake a public consultation, usually accompanied by a draft code, before issuance. This is an extremely valuable exercise and a practice that is strongly recommend. The difficulty with drafting codes of practice is that, although PCO staff may be experts in the legal technicalities of the Ordinance, it is often very difficult to envisage precisely how tenable a particular clause in a code will be when applied to a specific sector, industry or activity within the community. Secondly, public consultation allows us to 'test market' some of our ideas and obtain feedback on them.

- The Ordinance empowers for the Commissioner to specify classes of data users e.g. public registers or list compilers, that may be required to file information regarding their personal data practices for compilation as a data users register, that would be accessible by the public.

- The inspection and approval of automated personal data matching procedures. This means considering any adverse effect upon the data subject as a consequence of large scale automated processes, that match personal data contained on two or more databases. The Commissioner must be convinced that the proposed procedures comply with a number of conditions. For example, whether such

matching is in the public interest and whether there are practical alternatives to matching procedures.

- Inspection of the personal data systems of data users. Coverage here includes private sector organisations as well as government departments and statutory corporations. These systems are invariably computerised and IT specialist skills are required to undertake compliance checks.

- Power to hold public hearings and summon witnesses for examination

- Power of entry on premises for the purpose of inspection of personal data systems or investigation of complaints

- Power to issue enforcement notice to compel compliance, non-compliance of which carries criminal sanction

- To promote awareness and understanding of the Ordinance. We believe that promotion, education and training have been, and continue to be, invaluable tools in disseminating a rather complex message. To date promotional activities have ranged from main media campaigns e.g. television and newspapers, to open training seminars, to road shows in large shopping malls. Continued emphasis will be placed upon this aspect of our work although the focus of future campaigns may shift to educational institutions.

- Liaison with our counterparts in other jurisdictions. The PCO's expertise is largely restricted to personal data privacy in Hong Kong and, because we have limited resources, it is very valuable to be able to draw upon the expertise of our colleagues in other countries. There is little point in reinventing the wheel in Hong Kong when others have amassed considerable experience in a particular aspect of privacy. While approaches in other jurisdictions may not be directly transferable to the Hong Kong context, studying developments elsewhere both informs our decision-making and contributes to a reduction in cycle times.

- Monitoring developments in the processing of personal data and IT that may have an adverse effect upon the privacy of the individual. The PCO is required to study the development of new technologies, and the products derived from them, that may be privacy invasive e.g. smart cards and biometrics.

5.4 This is not a comprehensive listing of the functions and powers of the Commissioner but it provides an indication of the areas and activities that comprise the greater part of the PCO' s day-to-day operations. Nonetheless, we are mindful of the massive strides made in IT and the need to balance respective risks and benefits insofar as they affect personal data privacy. A contemporary example of the balance to be struck between benefits and risks occurred in 2001 when the Immigration Department put forward a proposal to replace the existing Hong Kong Identity Card (which had been in existence since 1949) with a smart card. One of the concerns was that the smart card chip could be used to store personal data of government departments other than that of the Immigration Department. A second concern related to the prospect of the private sector making representations to extend the original function of the smart card to commercial applications. In both instances the PCO were of the view that these concerns hinged upon what is termed "function creep." Simply, that the original purpose of the identity card would come under pressure to deliver a host of supplementary applications. If that were the case then there would be an absolute need for the Immigration Department to signal that intent well in advance and make subscription to any new function the subject of consent. This would inform the choice of the community and individuals could then decide whether it was in their interests to opt-in or opt-out of any supplemental applications given to the card e.g. driver licence details, library access and borrowing facilities etc.

5.5 While not opposed to the issuing of a smart ID card the PCO was quick to express its concerns which were conveyed to officials in the Immigration Department. The PCO also made the recommendation that the smart identity card project be subject to a Privacy Impact Assessment ("PIA") which would investigate the privacy issues, report on them, and make recommendations. This suggestion was taken up and the substance of the consultant' s PIA report has been incorporated into subsequent phases of the project.

5.6 This is merely one example of the new challenges confronting personal data privacy in Hong Kong. Those challenges demand that the PCO remain vigilant around the privacy impact of new technology that is invariably sold on its benefits. It is our duty to give voice to the associated risks so that the community can debate the issues and come to an informed decision. However, this example also gives the flavour of the way in which the PCO prefers to work on new projects and in the development of policy. The partnership in privacy approach has a number of attractive features and we have found it to work well resulting, we believe, in a better solution to

privacy-related concerns. We also feel that the approach affords mutual learning and understanding of the respective positions of the parties and this too is beneficial to discussions and in working towards a mutually acceptable outcome.

6 The Data Protection Principles

6.1 The judgements made by the PCO in the course of performing its duties, are anchored in a set of tenets that are referred to as the Data Protection Principles. These principles reflect the essence of the Ordinance and serve as the foundation for personal data privacy rights in Hong Kong.

It may be instructive at this point to briefly review the data protection principles.

DPP1 – The Purpose and Manner of Collection
This provides that personal data should only be collected by means that are lawful and fair for the purposes related to the functions or activities of the data user. In addition, the data collected should be adequate but not excessive for the purpose(s).

DPP2 – Accuracy and Duration of Retention
All practicable steps should be taken to ensure that personal data are accurate having regard to the purpose(s). If the personal data are believed to be inaccurate, the data should not be used until it has been corrected. Alternatively, the data should be erased. In addition, personal data should not be retained any longer than is necessary for the purpose(s).

DPP3 – The Use of Personal Data
This principle provides that personal data should only be used for the purposes for which they were collected, unless the data subject consents to a change in purpose. Furthermore, the prescribed consent should be express and given voluntarily.

DPP4 – The Security of Personal Data
All practicable steps should be taken to ensure the protection of personal data against unauthorized or accidental access, processing, erasure or other use, where these could cause harm to the individual. The principle also provides for the protection of secured storage, accessing and transmission of data.

DPP5 – Information to be Generally Available
This principle deals with transparency and provides for openness by data users about both the kinds of personal data they hold, and the main purposes for which personal data are used.

DPP6 – Access to Personal Data
DPP6 confers upon the data subject the right to ascertain whether a data user holds his/her personal data and to request access and correction of that data. Should the data user refuse to comply with the request then the data subject is entitled to be given a reason for the refusal.

7 Setting Course: The Early Years

7.1 I have already touched upon the fact that as our day-to-day business requires a heavy commitment of resources to dealing with enquiries and complaints the PCO, of necessity, became an operations-driven organisation. Expectations around public and private sector service providers in Hong Kong are high. That aside, the PCO is expected to maintain publicised service pledges that are an important measure of its productivity. The PCO does not, at present, possess the power to prosecute in a criminal court. However, legislative amendments are now being considered to extend this aspect of the PCO's enforcement capability.

Although this emphasis was right at the time we soon realised that our operations-driven approach would need to be complemented with a rather more 'customer-driven' approach towards the community. This approach involves the work of our Corporate Communications and Policy divisions which are respectively concerned with formulating and devising effective communications strategies and determining our approach towards, and development of, privacy projects.

7.2 Corporate Communications

On the basis of what we knew at the time we identified a number of issues relating to effective communication with the community. These may be briefly summarised as follows.

- Personal data privacy as a concept is not an easy notion to communicate especially when there is a need for it to be demarcated from privacy in a more generic sense. So, one of our first tasks was

to embark upon community education as the vehicle for conveying a better understanding of personal data privacy and attendant rights.

- Borrowing from proven marketing techniques we then began to sell the benefits of personal data privacy rights. In building our arguments we sought to inform the community of the value of personal data and how the less scrupulous might exploit it given the opportunity. For example, at the time there were reports of retailers retaining a person's ID card for hiring a bicycle for a day. This eventually led us to taking measures to curb such practices.

- Thirdly, we were aware of the fact that in the community we were largely an unknown entity in terms of role and the functions we perform. Clearly this meant that we would need to concentrate upon creating and building awareness. This was a consistent aspect of our communications strategy over the first five years or so.

- We also knew that we would need to correct some mis-understandings of our role and powers that had spontaneously developed in the community because the public were largely unaware of the type of privacy issues we were, or were not, authorised to investigate.

- This latter point also led us to the realisation that some people might perceive the PCO as all things to all people as long as the word privacy was in the title. To some extent this problem remains with us and we recognise that we must both influence and manage public perceptions. In some instances this means educating the mis-informed and revising expectations downwards, which can be problematic as it can frustrate an individual complainant. Naturally we would prefer those who consume our services to go away as happy and satisfied customers. The inability to achieve that objective means that the PCO runs the risk of adverse word of mouth testimonial.

- In marketing our message we are relatively fortunate in that at a crude level our audiences are already segmented for us. They consisted of data subjects and data users. As a result we have tailored our communications programmes to distinguish between the needs of each and try to address those needs. In short, the message at one level is generalisable but at another level we have come to realise that such an approach will only yield a very limited understanding. We have accordingly eschewed the idea of a

homogeneous message and delineated it based upon the profile of the audience.

- Insofar as data users are concerned we still see the need to sustain our influencing skills in selling the advantages of a privacy-compliant organisation. As mentioned, we have our critics and in the business community they can be both vocal and powerful. We have sought to better understand and address their needs by working closely with them. However, the issue today is not so much one of width but depth. We have made good progress in terms of persuading government departments and larger employers of the value of the privacy-compliant organisation although we are conscious of the costs incurred and the fact that, in a laissez faire economy such as ours, the tradition dictates that government should err on the side of being hands-off in its approach. Nonetheless, many government departments have committed to training related to personal data privacy and to delegating related responsibilities to a nominated individual. The same is true among larger employers in the private sector. Those who handle large quantities of personal data such as the financial services sector invariably have a Data Protection Officer/Manager and it is from their ranks that the PCO recruits members for the Data Protection Officers Club.

  The real issue now lies not so much with larger data users but with the smaller organisations, notably SME's, and this is where we will have to focus resources in the future given that the Hong Kong economy is an economy of small firms.

This listing provides some indication of our communications priorities.

7.3 Among data subjects the need has been to promote awareness and interest by resorting to educational programmes to create realistic expectations in the community. Among data users the requirement has also been to educate and facilitate privacy compliance which has meant influencing corporate attitudes and behaviours. Again, we have sold the benefits of a privacy compliant organisation involving a number of platforms. These can be briefly summarised as follows.

- Good personal data privacy practices amount to an investment in consumer confidence and this is an important step in the process of building repeat buyer behaviour and long term loyalty. To that extent best practices in the management of personal data exemplify a

commitment to customers' needs and may remove some of their anxieties.

- ❒ Good personal data privacy practices are one means of adding value to products and services. To my mind marketers have not realised the full potential of this statement. We know in Hong Kong, as elsewhere, that consumer doubts in the B2C market regarding online vendors privacy practices is a major impediment to shopping.

- ❒ Good privacy practices are indicative of good corporate governance and, after the debacles of recent years, there should be no doubt about the value corporate decision-makers should attach to good governance.

- ❒ Good privacy practices make a contribution to enhancing the value of intangible assets e.g. relationships with stakeholders and corporate image.

- ❒ Why invite customer complaints, possibly litigation, when good personal data privacy practices can significantly reduce the chances of this sort of action and avoid accompanying costs?

7.4 There is clear evidence that these appeals have been successful in influencing corporate practices concerning the management of personal data. Many large employers in Hong Kong have responded positively and made an investment in carefully drafted personal data policies, related practices and staff training.

7.5 **Policy**

From the outset the PCO realised that it had the choice between the carrot and the stick. We made the conscious decision to favour the former over the latter because we did not want to coerce data users into compliance with the threat of legal action. We feel it to be much preferable to win converts to the cause of personal data privacy and have accordingly sought to influence behaviours in that way. The alternative would have been a more combative approach that may have resulted in confrontation and an estrangement between ourselves and data users. In my opinion we made the right decision for the right reasons and this has paid dividends. The most obvious of these is that our preferred modus operandi has won us friends and made it easier for the PCO to enlist the support of data users in

developing pragmatic solutions to privacy-related issues. In the short/medium term I cannot see that we will abandon this decision.

7.6 Generally our view towards developing privacy awareness and compliance has been to engage a conciliatory and consultative approach. In a number of instances we have taken this one step further by isolating expert, interested or affected parties and entering into a partnership with them. We have deliberately sought to gain the trust and support of third parties in the development of privacy policies especially those that have serious and far reaching implications e.g. the amendments we recently made to our Code of Practice on Consumer Credit Data[3]. In this particular case we established a joint working party to study the industry and privacy-related issues. I will revert to this particular example in rather more detail later on.

7.7 If there is a phrase that you will hear time and again in the PCO in our internal discussions, committees and brain storming sessions it is the need to 'strike an appropriate balance.' Quite what that balance looks like at the outset is not always immediately clear but it is something that we are very conscious of in our deliberations. I suppose this is because in Hong Kong we regard ourselves as privacy pragmatists rather than privacy purists. Again, I think in our context that stance is the most fitting of the two quite simply because the 'remedies' that come out of it are less severe, less extreme and less likely to alienate.

Perhaps the best way for me to illustrate 'striking an appropriate balance' is by making reference to one of our current projects which involves the development of a Code of Practice on Monitoring and Personal Data Privacy at Work. I do not need to lecture my friends in the UK privacy community on this matter as they have rich first hand experience of the problems and pitfalls associated with developing such a code. Nonetheless, I think that in the face of mounting surveillance in the workplace, and elsewhere, Privacy Commissioners are justified in seeking to lay down some ground rules that give the semblance of balance to the employer/employee relationship.

In seeking to develop such a code we have spoken with employers and their representatives and conducted a public consultation exercise. What we found from that exercise was that there was general support for some sort of guidelines or a code. However, this view is not shared by a number of large, very vocal and powerful employers who, in principle, are strongly opposed to this PCO's initiative. Indeed, they are on record as saying that

[3] Details of the amended Code, the draft consultation document and consultation report can be viewed at the PCO's website http://www.pco.org.hk/english/ordinance/codes.html

such a code is largely redundant a) because there is no evidence of mischief on the part of employers and b) because the employee's expectation of privacy is greatly diminished in the context of the workplace.

This opposition has not deterred us in our endeavours but it has made us mindful of the posture we have chosen to adopt towards the community. The challenge before us then is to strike a balance between the employer's right to manage the assets and resources of the business and the privacy rights of the individual employee. In the other example cited, amendments to the Code of Practice on Consumer Credit Data, the balance was between the public interest and the privacy rights of the individual.

7.8 I imagine that if the PCO were a business then what we term policy would be akin to an R&D or new product development function. If that were the case then I think, rather like industry, one would look to ones consumers, the community, for ideas regarding privacy projects worthy of investigation. We remain open to suggestions from our partners in privacy and have responded to them on a number of occasions. For example, our work with professional bodies resulted in one of them suggesting the development of a Code of Practice on Human Resources. The request here was to assist those in the HR field in applying the provisions of the Ordinance that, admittedly, are less than user-friendly. The PCO benefited greatly from the support and co-operation of the HR profession by having access to practitioners who assisted us in determining the scope of the code and the detail we should go into e.g. the range of HR situations in which personal data might be handled by an employer. We have never claimed to be omniscient on matters relating to personal data privacy and that is by no means the case in understanding the inner workings and idiosyncrasies of a particular profession or business sector.

7.9 I hope I have been able to convey both the range of communications objectives we established for ourselves and the essence of our partners in privacy approach. However, setting objectives is one thing, and the easier part, attaining them quite another. As a publicly funded body I believe it is imperative that we demonstrate that we are utilising the resources at our disposal both efficiently and effectively. This means demonstrating our performance and subjecting it to public scrutiny.

8 Taking Stock of Progress to Date

8.1 It has been said that if you can't measure it you can't manage it. I believe therefore that we need to be accountable for doing what we say we will do.

This means that we have had to develop some indicators among data subjects and data users of the impact our strategies are having upon public awareness and compliance. To do this the PCO commissioned the Social Sciences Research Centre at The University of Hong Kong to undertake a series of studies of perceptions held by data subjects and data users towards personal data privacy. The baseline survey was conducted in 1997 and repeated over the following four years. In 2001 the PCO had five years of comparable data to work with. By then the trends were pretty much established so we discontinued this exercise because the value of the data yielded was only of marginal utility[4].

8.2 The annual opinion survey yielded information that was valuable in at least three ways. Firstly, it assisted the PCO to get a fix on its position. Secondly, it enabled us to track perceptions towards our work on a year-to-year basis. Thirdly, it offered a means of testing new ideas and policy initiatives. For example, the Code of Practice on Human Resource Management was launched in April 2001. Some time later our consultants asked data users whether this code had been helpful to employers and HR professionals in terms of applying the provisions of the Ordinance in the context of contemporary employment. We were gratified with the results obtained from the survey which vindicated the time and money invested in the project.

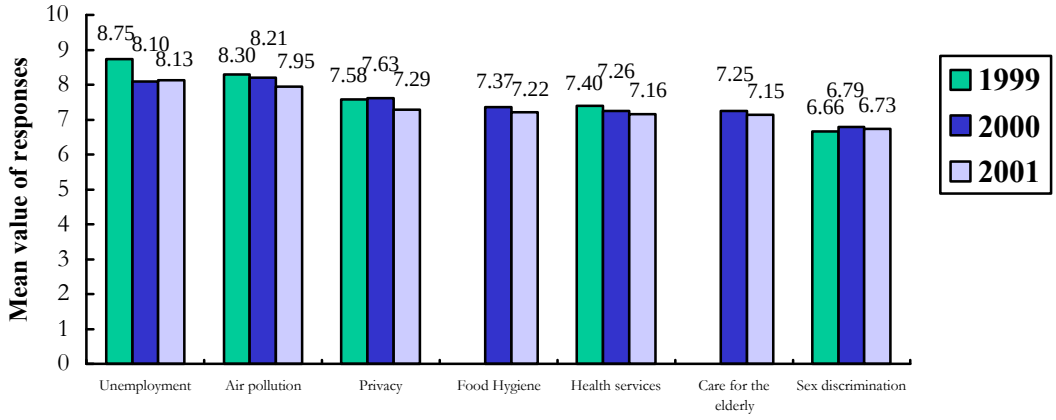
[4] By way of a footnote to this the PCO decided in 2002 to change the focus of the survey from the big picture to something more specific. In that year we investigated public perceptions towards surveillance cameras in public places. A synopsis report of the findings of the survey can be found on the PCO's website at http://www.pco.org.hk/english/publications/opinionsurvey.html

8.3 I would like to take this opportunity to give you some indication of what we have learned about our efforts to popularise personal data privacy, create awareness and encourage compliance in the community.

DATA SUBJECTS FINDINGS

- **The Importance of Privacy in Relation to other Social Policies in Hong Kong (Figure 1)**

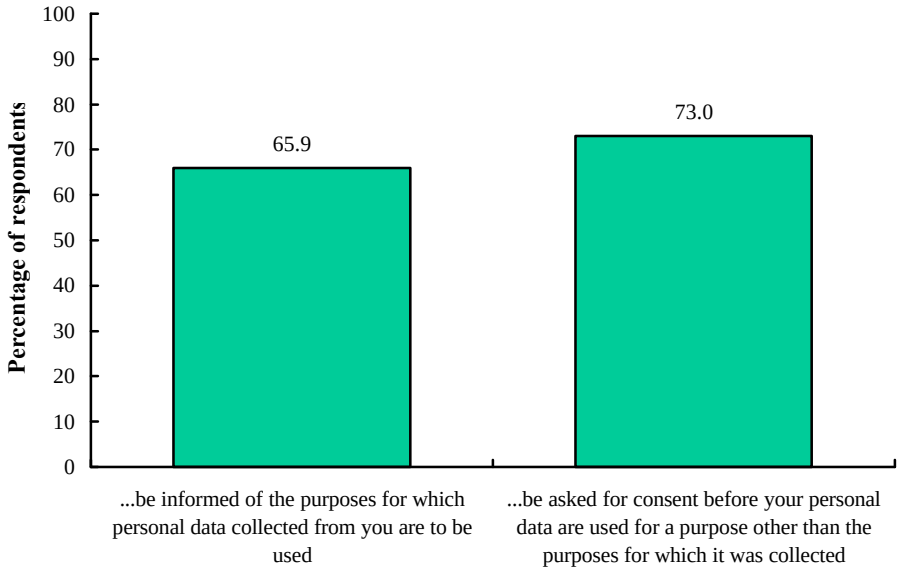
Figure 1 – The Importance of Privacy as a Social Policy Issue



Privacy comes behind unemployment [which has increased significantly in recent years] and air pollution but consistently scores high marks in terms of the value attached by respondents to this particular social policy.

❒ **Awareness of Personal Data Privacy Rights (Figure 2)**

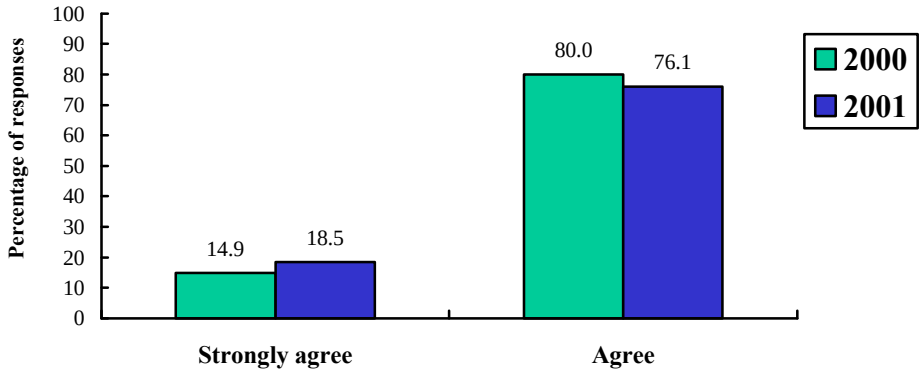
Figure 2 – Are you aware that except when used for law enforcement or national security, you always have the right to …



Although the community is better informed about their personal data privacy rights it is only fair to say that they do not find these rights easy to articulate, unless prompted. This is unsurprising because, with the exception of ‘high interest groups’, it is improbable that members of the community would carry the DPP around in their head.

❒ **General Awareness of Data Privacy Issues (Figure 3)**

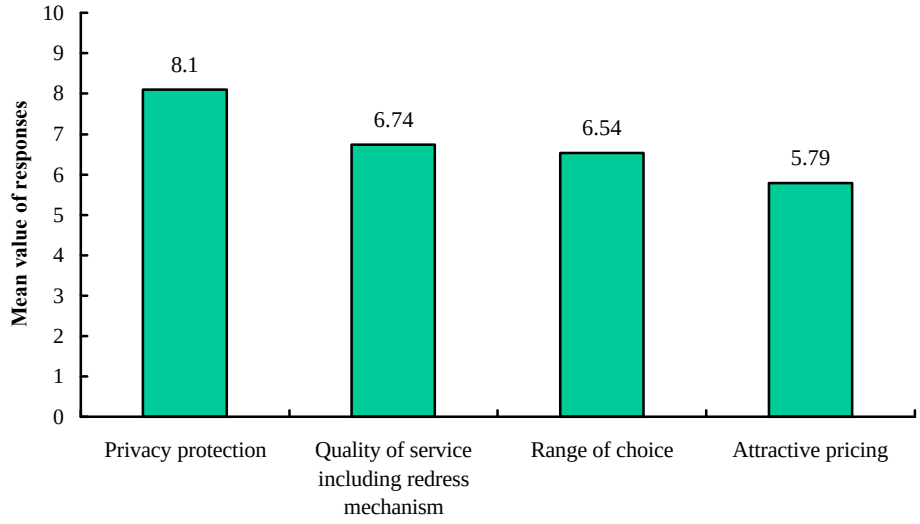
Figure 3 – Has the PCO increased community awareness of personal personal data privacy issues?



Some comfort can be taken from the fact that the PCO is getting its message across to the community through the combined efforts of promotion, education training and the Data Protection Officers Club. Nonetheless, we have detected that there are still a few resistant outcrops and that we have some way to go in informing certain sectors of our society, notably the elderly and less well educated.

❒ **Public Concerns Remain ~ Principally in the E-Privacy Arena (Figure 4)**

Figure 4 – The Importance of Factors in Making Purchasing Decisions on the Internet

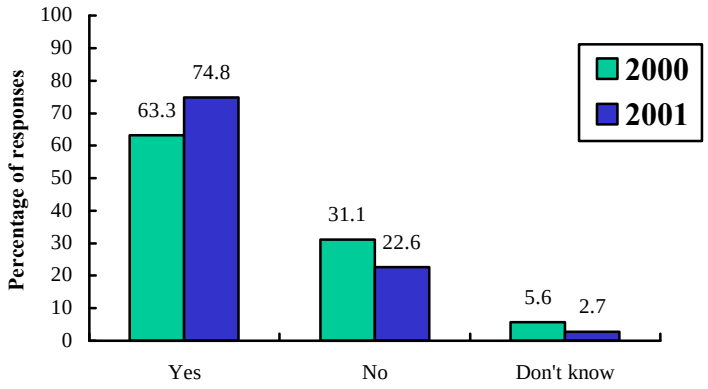


Earlier I mentioned that on-line purchasing amounts for a very small proportion of total consumer spending in Hong Kong. One explanation of this behaviour is provided in Figure 4. Our research into privacy-related issues and the Internet indicates that there is a large measure of concern in the community regarding the control web users exercise over personal data divulged online. Unless, and until, service providers address online privacy issues and provide online solutions to effectively address those issues then low levels of trust and confidence will prevail in the B2C sector.

DATA USER FINDINGS

- **Responses by Data Users Towards Compliance with the PD(P)O (Figure 5)**

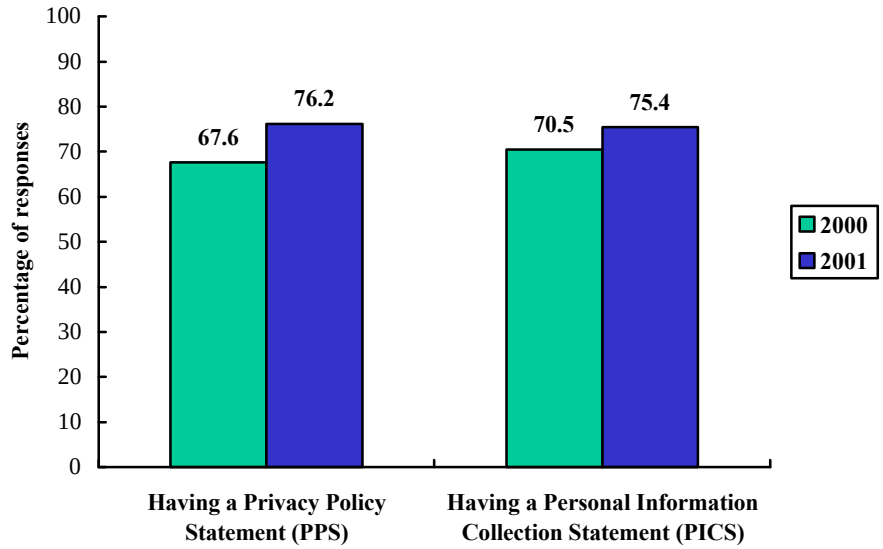
  Figure 5 – Have data users formally adopted written policies to comply with the ordinance?



It has always been our practice to encourage data users to commit their personal data privacy policies to writing so that they are readily available to employees, customers and other stakeholders. Progress has been made on this front although the task has been more problematic among online businesses than conventional 'bricks and mortar' businesses.

❒ Informing Data Subjects of Compliance with the PD(P)O (Figure 6)

Figure 6 – Possessing a Privacy Policy Statement[5] and Personal Information Collection Statement[6]



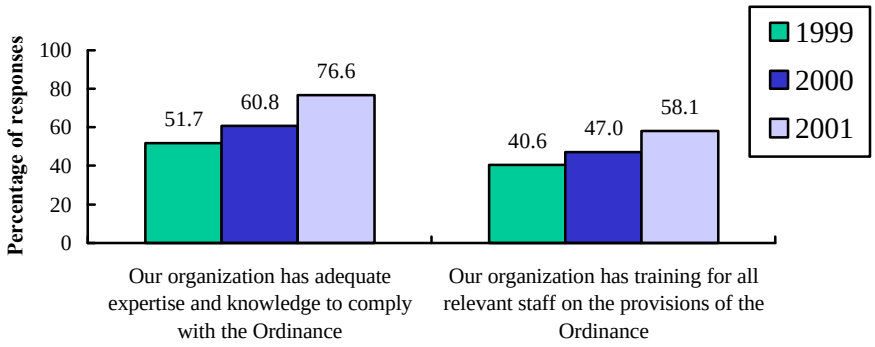
Over the years the PCO have sought to encourage data users to comply with the provisions of the Ordinance by formulating and disseminating a PPS and PICS. There has been a steady increase in the percentage of data users issuing such statements and this is invariably the case with medium and large-scale organisations. The challenge right now is to migrate that behaviour to small organisations that handle personal data.

[5] A Privacy Policy Statement (PPS) is a general statement of an organisation's policy and practices in relation to its collection, holding and use of recorded information about individuals. Under the Ordinance data users are required to ensure that their policies and practices in this regard can be ascertained by other persons.

[6] A Personal Information Collection Statement (PICS) is a statement given in compliance with the requirements of the Ordinance to notify individuals of certain matters when collecting such information from them. That is, it is a statement of a certain limited content given in relation to specific collections of recorded information from individuals about themselves.

❒ **The Provision of Training by Data Users for their Staff (Figure 7)**

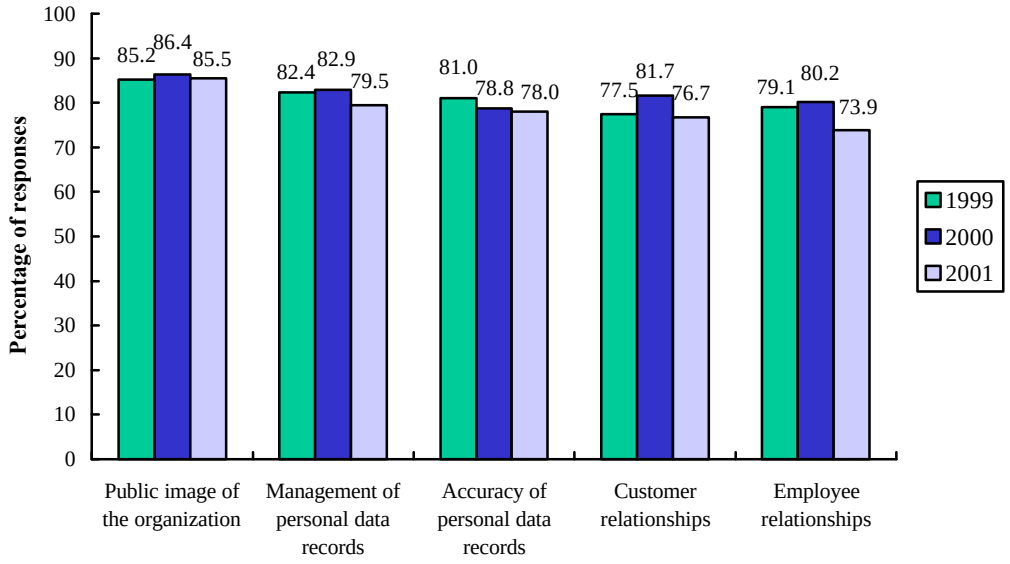
Figure 7 - Data Users Training Provision for Staff Preparedness for the Ordinance (Aggregated Agree/Strongly Agree Responses)



It has been gratifying to learn from successive surveys that more and more data users are allocating the responsibility for personal data privacy to a designated person – a Data Protection Officer ("DPO"). One of the duties of a DPO is to create awareness among staff of the implications of the Ordinance and keep them current on developments. This is most effectively achieved through the provision of training sessions and staff seminars. To support this organisational commitment the PCO's Data Protection Officers Club provides a regular forum in which to update learning from current complaint cases, offer refresher training and learn from expert speakers.

❒ **The Long Term Benefits from Compliance with the PD(P)O (Figure 8)**

Figure 8 – Long-term Benefits to Data Users of Compliance with the Ordinance (Aggregated Agree/Strongly Agree Responses)



These findings are important in that they enable the PCO to cite evidence that reflects the perceptions of data users towards compliance with the Ordinance. Clearly we do not wish to be regarded as a bureaucratic imposition upon organisations, especially businesses. Fortunately, compliance is generally regarded very positively in terms of the long-term benefits and goodwill it confers upon the organisation. This would tend to suggest that compliance is, perhaps, less a cost, although clearly there are costs, and more of an investment in the organisation's image, customer/employee relationships, and best practices insofar as the management of personal data are concerned. The PCO can argue, with some justification, that compliance with the provisions of the Ordinance adds value to data user organisations.

Although I have not done justice to much of the data we have at our disposal our most recent survey findings give rise to guarded optimism in terms of the PCO's efforts to build a culture in Hong Kong that respects personal data privacy. There are no grounds for complacency because there is much to be done in the area of educating children, young adults, senior citizens and small businesses. This of course makes no reference to the emergent challenges to personal data privacy posed by the diffusion of new technology, and the ramifications of the unimaginable events of 11 September. I will offer my interpretation of those events towards the end of this paper.

9 Consolidating the Gains

9.1 If the past six years can reasonably be labeled the pioneering phase in the PCO's development then I think the next five years or so will constitute a period of consolidation. By that I mean that the PCO will seek to reinforce existing understanding and expand the knowledge of the community in relation to personal data privacy issues. In our view one of the most important tasks will be to ensure that the community truly understands the formidable threat to privacy posed by technology. No one should be in any doubt that while technology can be applied to serving the privacy interests of the individual its greater focus has been upon privacy invasiveness. It has been argued that the imbalance between privacy and technology is so great that it will hasten the demise of privacy. Unless one is a total recluse it is virtually impossible for the individual to do anything but leave data trails relating to daily exchanges and events. This means that the levels of privacy enjoyed today are a shadow of the levels of privacy enjoyed say ten years ago. This trend will continue at an accelerating rate and the community needs to be informed of this so that they can exercise some moderating influence or at least demand that data users consider the privacy implications of new products and services. Nonetheless, the likely shape of things is that technology-driven change will create greater convenience and consumers will trade privacy for this. The need to inform the community of this rather uncomforting scenario is a responsibility we must assume.

9.2 It is against this backdrop that the PCO will endeavour to reinforce the gains of the past by seeking to instill a respect for privacy in all quarters of the community. The following summary offers some insights into the sorts of activities that will preoccupy the PCO over the course of the next five years.

- Emphasis will be placed initially on public bodies, and then upon the private sector, to make Privacy Impact Assessments ("PIA") a constituent element of any project or initiative that could have a material effect upon the community. Attention here will focus upon encouraging a proactive approach to privacy impact and the need for it to be regarded as a 'must have' aspect of project management rather than a 'nice to have' element or casual afterthought. As indicated, advances in surveillance, biometrics, 3G mobile phones, wireless computing, smart cards etc. will mean that those developing products for these markets must be made aware of, and respond positively to the privacy-related issues associated with the

technologies that make these applications possible. In short, data users should go out of their way to inform consumers of the consequences of using new applications technology in terms of personal data privacy. In an ideal world one would like to see privacy mentioned as a product dimension featuring in promotional literature and operator manuals. Indeed, it is quite possible to envisage 'privacy protective features' as an integral part of a consumer product's selling proposition.

In the public sector I think we will seek to encourage government departments and agencies to make the findings of PIA studies available. Not only would this practice uphold the principle of transparency, to which the HKSAR government is committed, but it would also inform opinion and allow for healthy public debate of the issues.

- Section 8 of the Ordinance empowers the Commissioner to "examine any proposed legislation that the Commissioner considers may affect the privacy of individuals in relation to personal data and report the results of that examination to the person proposing the legislation." We have been diligent in discharging this duty and our recommendations have led to amendments of legal provisions before and after a Bill has reached the Legislative Council for consideration. In future we will try to encourage government departments to build privacy into their thinking when developing new policies, taking new initiatives and drafting legislative proposals. Once again this implies a proactive approach rather than an ex post facto response. Getting to this goal will necessitate educational efforts, a change in thinking and a modification of administrative processes. One is hopeful that if these changes occur then this will inspire the private sector to make similar adjustments.

- Through our promotional activities, especially those directed towards schools, students and younger people we will seek to make privacy what I would call an autonomic response i.e. second nature. In Hong Kong secondary school students are required to study a subject titled Economics and Public Affairs. This is an eclectic syllabus that looks at economic, political and social issues. Some well-established government agencies are very active in promoting their cause to this target group e.g. The Independent Commission Against Corruption. I feel that if we can get privacy included as part of that syllabus, and reinforce this with promotional events such as roadshows and competitions, we will manage to influence young

minds and ultimately this will lead to behaviours that respect privacy. There are models for this approach that have worked well in Hong Kong in terms of changing attitudes and behaviours towards the environment, littering and drugs. I can only see benefits deriving from this initiative because the younger set will influence the behaviour of others.

The hoped for outcome is that young people will attach considerable value to personal data privacy, become more knowledgeable about their rights and understand how and when they should exercise those rights. To me this seems a win/win situation. Personal data privacy stands to become a valued civil right among the young and if value is established for privacy at an early age then this is something that people are likely to carry with them for the rest of their lives.

Taking this to the adult level there are already signs that the populace is beginning to become vocal in representing privacy rights that may be perceived to be under threat. For example, some three years ago the Immigration Department decided to replace the existing identity card with a smart card. This seemed a reasonable proposition when presented (given that Hong Kong has had identity cards for its citizens since 1949) but gradually, as the community began to understand more about the potential capabilities of a smart ID card, the level of public debate and, in some cases opposition, rose. Of course the concerns were around the security aspects of the card i.e. who would know what about the holder and how might they use that knowledge for unauthorised purposes. Secondly, concerns were expressed about the phenomenon of "function creep."

The media exposure given to respective arguments by experts and the lay man alike heightened awareness of the privacy impact of issuing a smart card. Essentially this was a positive development because it resulted in the Immigration Department subjecting the project to a robust PIA over four stages and agreeing to submit the programme when completed to an independent privacy compliance audit to ensure that the integrity of system safeguards have not been compromised. Strong community view had been expressed that the audit report should be placed in the public domain which could only be good for transparency and privacy.

In another example early last year [February 2002] privacy concerns were at the centre of another public debate concerning the proposed installation of police surveillance cameras in a public place

frequented by people seeking a good time in a locale that is crammed full of bars, clubs and restaurants. The issues were eventually debated by the Legislative Council which added fuel to the fire. In the face of the concerns expressed the police withdrew its funding application and suspended the trial installation of cameras[7].

What these incidents illustrate is that the community are both more vocal and more active in drawing attention to privacy-related projects that are brought to their notice. This is an important development and one that we would wish to encourage because it suggests that there is a certain penchant among the general public for 'policing' privacy. In both instances the concerns raised have acted as a countervailing force and this has given rise to a more careful consideration of privacy issues by the principal protagonists. There is learning in all this and one is hopeful that the learning will reduce the incidence of projects getting to an advanced stage without first having considered their privacy impact. In these particular instances prevention seems preferable to cure and certainly a lot less costly.

- Finally, to complement our focus on consolidating the gains in the public sector it is only fair that we should apply the same logic to the private sector. We have seen promising developments here of late and I think that, once again, the media exposure and public debate has been very beneficial to the privacy interests of the community. It is to be hoped that recent examples will give impetus to the private sector to consult the PCO when embarking upon large-scale projects that have significant consequences for the community.

- We will be seeking to leverage the gains made in a landmark exercise this year by using it as an illustrative example of how the partnership in privacy can be mutually beneficial to those involved. The development that I am alluding to involved approaches made by the financial services sector in Hong Kong to the PCO requesting that consideration be given to credit providers having access to limited positive credit data of their customers. For this to happen the provisions of the Code of Practice on Consumer Credit Data ("the Code") would have to be amended. Our view was to look at this request in the context of balancing the public interest - transparent

[7] Subsequent to this incident the PCO investigated the phenomenon of surveillance cameras in public places. The research design involved focus group interviews, a household survey administered by telephone and in-depth interviews with camera operators. A synopsis report of the findings of that survey can be viewed at the PCO's website at http://www.pco.org.hk/english/publications/opinionsurvey.html

and stable consumer credit markets - and the personal data privacy interests of the individual. To assist the PCO in coming to an equitable solution in what was a high profile case involving controversial issues the PCO set about mapping the dimensions of the problem and examining the constraints under which those in the financial sector were operating. In this instance, we were approached by the Hong Kong Monetary Authority and the Hong Kong Association of Banks. Subsequently, we considered both public and private interests important enough to justify a joint working group comprised of the respective parties and it became an exercise in partnership.

I feel we responded to the situation well by adopting the view that any outcome would best be served by the PCO not acting alone, but in conjunction with others. This we did over a period of around six months, meeting regularly. In those meetings representatives of the financial services sector described the acute problems of loan default and credit card delinquency in the consumer market, a situation which they argued was aggravated by a lack of ability to access necessary financial information of individual borrowers. In addition, they laid out their requirements for having access to additional personal data disclosure by customers, justified them and explained how the proposed scheme would operate via the intermediary of a credit referencing agency.

Having listened to the arguments we began to look at the code with a view to making amendments that would enable credit providers access to limited positive data of their customers. However, our conditions were that a multi-tiered set of safeguards must first be put in place before the scheme could commence operations. We also insisted that the scheme be subjected to independent auditing to ensure that users were compliant with the conditions agreed to.

I have overviewed this project which was completed in June of this year because it is a graphic illustration of the way in which positive steps were taken by institutions representing arguably the most important and powerful sector of our economy: financial services. The learning for all of us was that the model and the iterative processes it embraced were very beneficial to facilitating an optimal solution that earned the respect of all parties. I don't think that job would have been nearly as well done if the financial services sector had not approached us and been very candid about their needs. I

also think that the amendments we made to the Code benefited from the information provided to us during our working party meetings.

It is therefore our intention to encourage the private sector to make similar approaches in the future. Such an approach will work towards outcomes that we may not officially pioneer, but find agreeable from a broader personal data privacy viewpoint when presented with cogent and valid justifications. This is another tool in the kit with which to consolidate our gains, heighten awareness of privacy issues and encourage compliance among private sector data users. Our door is always open to such approaches, indeed we welcome them, because they are indicative of the value attached to privacy, and the respect accorded to the rights of the individual among private sector organisations that handle personal data. I feel this way of doing things is more likely to lead to solutions that accommodate privacy considerations rather than run roughshod over them.

10 The Road Ahead

10.1 Insofar as the future is concerned, at least during my term as Privacy Commissioner, we will seek to inform and educate the community about two issues that are going to have a major impact upon our thinking and policies. The first of these relates to what has been termed the Surveillance Society. It is increasingly evident that this concept is no longer the exclusive preserve of fiction writers. On the contrary, it is at risk of becoming a reality in the near future. The most extreme manifestation would be a total surveillance society in which virtually everything is known about everyone no matter where they may be at any given point in time. The second relates to the growing call for trans-border data flows to be regulated in the context of rapidly expanding global trade. In the relatively recent past this issue has moved from being on the local agenda to one that is now actively being investigated by APEC (Asia-Pacific Economic Cooperation) a trade and business forum in our region. There are good reasons for this, not the least of which is that events have largely over taken attempts to establish some framework in which trans-border data flows are subject to controls be they statutory or self-regulatory.

The Surveillance Society

10.2 Both the direct and indirect evidence we have in Hong Kong is that surveillance is an increasingly prevalent trend in which the only way is up.

In the most extreme situation depicted the inevitable conclusion is that our personal freedoms and way of life are at grave risk of being irreversibly altered. In Hong Kong, there is no doubt in my mind that an increasing number of citizens are subject to surveillance, in private and public places, without them necessarily realising that is the case[8]. Not only are levels of surveillance increasing but as technology, used primarily for military or security purposes, migrates to consumer product markets it is inevitable that surveillance, in a multiplicity of new forms, will proliferate. What is more the data collected will be used in conjunction with biometrics and digital recognition databases for questionable purposes.

These levels of surveillance will be intrusive of privacy in its broadest sense and not just personal data privacy. While some in our community have sounded the warning I generally I do not think that, at this stage, the public at large are fully informed of such developments, neither do I think that they fully comprehend their implications, not to mention that the means by which some of these monitoring devices are marketed tend to pander to the curiosity of some members of the public. In these circumstances the PCO must remain vigilant, abreast of developments in surveillance and communicate any concerns to the community. Only in this way will the public come to an informed opinion and on the basis of that make an informed choice.

If we assume that choice is an option then the individual may be able to decide the trade-off between privacy and surveillance. However, I suspect that the inducements given for monitoring real time personal data will be made appealing. Again that is a matter for the individual who will be influenced by many factors. For our part we have a duty to signal such developments to the community and present the privacy arguments to them. If I were to have my way what I would like to see is for public opinion to be mobilised in such a way that the acquisition of personal data, by one means of surveillance or another, would be subject to the countervailing power of that expression.

However, I have to admit that certain circumstances will virtually rob the individual of any such power. The most obvious example being in the workplace. Our office has some experience of this context having put out a draft Code of Practice on Monitoring and Personal Data Privacy at Work

[8] For example, the advent of the mobile phone with camera function has resulted in up-market Health Clubs and Fitness Centres in Hong Kong banning the use of these devices because they are invasive of the privacy of members and pander to the needs of the voyeur.

("the Code") for public consultation[9]. Prior to embarking on that exercise we undertook some research into surveillance in the workplace and found that, of the data users we surveyed [all of them employers], 66% had installed one or more forms of surveillance at the workplace and 34% had installed two or more. However, less than 20% had a written policy statement informing employees of the purposes of collection. I am bound to say that I think that the microcosm I have described is replicated many times over on a global scale. And there is more to come.

In view of what I have said I think that there is every reason for us to be alarmed at the prospect of the surveillance society becoming a reality in a relatively short space of time. I say that not simply because of the variety of surveillance devices available and the growing pervasiveness of surveillance but because of something that, hitherto, I have not brought into the picture. That something is international terrorism and the counter-terrorism measures now in place, or being put in place, by many countries across the globe. Hong Kong is no exception to this predictable response. I do not propose at this point to review all the arguments but I do think we have to come to the realisation, fight as we may, that if it comes to a confrontation between national security interests and personal data privacy interests then the former will win the day. I think that there is clear evidence to support this in the headlong rush to get counter-terrorism legislation on the statue book if for no other reason than to reassure the public that ' something has been done.'

The important point may be lost in this headlong rush which is that the State and state agencies have, since the events of 9/11, conferred upon themselves unprecedented surveillance powers. While the man in the street may be inclined to accept this as the ' price one has to pay' at this point I do not think he knows quite how high that price is. Imagine, and it doesn' t take much imagination, security agencies in agreement with one another directly accessing passenger databases and cargo manifests of every airline in the world and using that data for intelligence purposes. In pursuit of the pre-emptive strike against potential terrorist threats I venture to suggest that an awful lot of personal privacy will be compromised. Is that the sort of world in which we wish to live even in the face of international terrorism? If so, then it was predicted many years ago.

I would press for a more reasoned response from governments especially in societies such as Hong Kong – and there are many of them – where the threat of terrorism is relatively low. That response would be less of a knee

[9] The draft Code of Practice on Monitoring and Personal Data Privacy at work can be viewed on the PCO' s website at http://www.pco.hk/english/ordinance/codes.html

jerk reaction and one that at least endeavours to give some protection to personal data privacy rights. However, I think that in all probability we will be forced to make some concessions and this will further erode the rights we enjoy. As such, the community needs not only to be prepared for this eventuality but to realise that it could be the shape of things to come i.e. the clock cannot be turned back and the protections afforded in the past will by no means be guaranteed in the future. At this stage I am unsure of quite how far this process of diluting or compromising privacy rights will go but if the threat of terrorism were to increase then it is possible to envisage a significant diminution of those rights in countries that have worked so hard to pioneer them. This seems a retrograde step and I feel that the international privacy community needs to work harder to ensure that governments listen to the counter-arguments rather than exhibit a disregard for privacy rights on the grounds that they must be sacrificed to the interests of national security. I fear if that is the case those rights will be lost forever and the community needs to be prepared for this. It is conceivable therefore that we may eventually be in the unenviable position of having to change community awareness and revise privacy expectations downwards.

Trans-border Data Flows

10.3 At the moment there is something of an impasse in efforts to satisfactorily resolve trans-border data flows primarily because the essential difference in approaches which range from statutory requirements to voluntary self-regulation. The best current example of this is the unresolved differences between the EU and the USA's safe harbour proposals. An interim report issued by the EU last year expressed some disappointment with the way in which the scheme was working at that stage.

In Hong Kong section 33 of our Ordinance deals with this aspect of personal data privacy but it is the only section which has yet to be enacted. This situation cannot be allowed to prevail much longer because we are already lagging behind developments in this sphere. Hong Kong is undergoing a protracted period of economic recession. In turn, economic adversity has meant looking for greater productivity and cost reductions. One such illustration of the latter has been for businesses to re-locate certain activities e.g. customer call centres, accounting functions and data processing over the border in neighbouring provinces where overheads and labour costs are considerably lower. Some of the operations of regional

countries have been moved further afield to India[10]. However, in both the instances cited there are, as yet, no reciprocal privacy arrangements between either the PRC or India with other jurisdictions. Neither is there any formal adequacy agreement with the EU. In both jurisdictions, national privacy legislation has not, as yet, as far as I am aware been enacted.

What in effect we have therefore is the rather unsatisfactory situation in which we suspect that personal data collected in Hong Kong, and protected by the provisions of our Ordinance, is removed to another place with no such protections. This situation cannot be permitted to prevail and we are currently reviewing the options open to us. On the face of it the most likely one would require those data users collecting personal data in Hong Kong to extend their responsibilities for the protection of that data to any jurisdiction to which it may be transferred to outside of Hong Kong. This provides less of a problem in certain instances such as New Zealand or Australia which have established privacy regimens. However, the same cannot be said of most countries constituting southeast and south Asia.

This is where APEC may step in and come to the rescue. Relatively recently that body has shown a good deal of enthusiasm for personal data/information privacy and has instituted a mechanism to try and forge agreements between member economies. At the moment it is seeking to draft a set of privacy principles that the twenty-one member economies can agree to abide by. Once these come into play the next logical step would be to develop a trans-border data flow protocol that would seek to apply protection to personal data transferred from one economy to another. Hong Kong, with a relatively well established privacy regimen, is playing its part in seeking to influence the outcome of APEC privacy initiatives which we fully endorse.

While accepting that the free flow of personal data is the lifeblood of business we feel that, in the first instance, the community is not fully aware of this practice and may therefore come to some erroneous view that personal data collected in Hong Kong is accorded similar protection elsewhere. As the practice of collecting personal data in one jurisdiction and transferring and processing it in another gathers pace there is an urgent need to address the consequences of such transfers. I think that in Hong Kong we will look to APEC to take the lead on this matter and work with them towards establishing procedures for bi and multi-lateral 'adequacy' agreements between member economies.

[10] In a BBC television report screened in Hong Kong on 20 June 2003 it was stated that there were already in excess of 400 call centres in India. The majority of these were investments were made by multi-national corporations.

It also occurs to me that if we do not address this issue in the near future we will not only expose ourselves to criticism from the community but potentially damage E-business opportunities. To do that would be to deny ourselves the advantages of this model of conducting business and thus not serve Hong Kong's economic interests. I am therefore keen for us in the forthcoming two years to stimulate public debate of the issues. Prior to initiating that debate I think we will conduct a survey to establish the prevalence of trans-border data flow among businesses in Hong Kong, the processes engaged and the safeguards taken to protect personal data once it is transferred to another jurisdiction. In that way we may, either on our own initiative or in conjunction with partner economies in APEC, be in a better position to formulate procedures and protocols to ensure data privacy is maintained.

I can also see the PCO having to monitor developments and modify the nature of its communications strategies. The community may need to be better informed about the implications for a society in which developments in technology have the potential to make surveillance a routine. We may also need to signal to the public that their expectations regarding personal data privacy may have to be re-framed in the aftermath of 9-11 and the resultant extension of legal powers accorded to state security and law enforcement agencies.

We will also be pre-occupied with seeking to come to a negotiated consensus with our colleagues in APEC to establish a multi-lateral framework for regulating trans-border data flows that ensures an acceptable standard of data privacy and at the same time helps to bring about economic benefits to the economies in the Asia Pacific region.

Based upon what information I have, and my intuitions, my best guess is that privacy will suffer losses on one front, surveillance, and gains on the other, trans-border data flows.

11 Concluding Comments

11.1 In common with other jurisdictions Hong Kong has faced its share of difficulties in operationalising data privacy law. Initially, personal data privacy did not register as an issue of great social concern in the community. Secondly, privacy was not high on the government's agenda as more pressing policy portfolios such as housing, education and healthcare were given priority. Thirdly, some elements of the private sector

went on the defensive by articulating the view that business would become less efficient, and consequently less competitive, if it were obliged to absorb the costs of compliance with the provisions of the Ordinance. However, over the course of the past six years I am pleased to be able to report that all three conditions have changed.

- Awareness of personal data privacy has grown significantly in Hong Kong and this has reflected in the value placed upon it. Today there is an informed discussion of privacy at all levels within the community and certainly in the media. This debate is very healthy because it acts as a check upon the excesses of the less scrupulous and serves as a reminder to those inclined to engage practices that are perceived to be invasive of privacy. If nothing else it is not good PR for a data user in either the private or public sector to have a complaint against them filed with the PCO and subsequently investigated, and the PCO is able to "name and shame" where public interest is involved.

- Secondly, government departments and bureaux have shown a lead in developing good personal data privacy practices and seeking counsel from the PCO. It would also be true to say that the Administration has consistently and generously funded our activities and that is still relatively the case in the present economic climate. In that respect we have been fortunate in the support we have received and are grateful for it.

- Business opinion has changed from scepticism to acceptance because we have been able to reshape earlier perceptions and because the business community now understands, and generally supports, both our privacy regimen and the benefits of being privacy compliant. Today data users in the private sector are less likely to adopt the view that compliance is 'just another business cost upon which there is no return.'

11.2 The mixed signals received by the PCO in the period immediately after its foundation had an air of apprehension about them. This apprehension emanated from established custom and practice around 'how we do business' in Hong Kong i.e. a laissez faire minimal interventionist economy. Note was taken of this apprehensiveness because it was our belief, and remains so, that privacy law can only operate effectively if it is understood and accepted by all sectors of society, especially the business community. Priority tasks therefore were to build relationships, and a culture that would nurture personal data privacy. At the time the thinking was that this

objective could only be achieved by a cultural shift in the collective consciousness of the citizens of Hong Kong. To make that shift the PCO moved ahead with the partners in privacy concept because this was felt to be the approach most likely to ensure the outcomes sought: awareness among data subjects and compliance among data users. This involved a process that was complicated. On the one hand we wanted to promote change but on the other we did not want to isolate any of the broad range of interests that typify a pluralist society. We were very much in the business of promoting change, and the concomitant of change is resistance to change.

11.3 On reflecting upon what has worked well in Hong Kong, and what has worked less well, we have come to an intuitive understanding about those principles that give definition to who we are, and what we do. In the early days there was an element of trial and error in our approach as the whole business of privacy was very new and there was no accumulated experience in Hong Kong to guide us. However, as time passed, the PCO managed to gauge the mood of 'the market' reasonably well and this influenced subsequent planning. Great faith has been invested in a number of fundamental principles that seem to have stood the test of time because we continue to adhere to them today.

- **Striking a Balance**
  In formulating and implementing privacy policy the PCO has frequently to walk a fine line between competing interests. An effective solution must acknowledge the interests of all parties. This means that an extreme or purist stance is less likely to appeal and less likely to result in a position that is reasonable, equitable and defensible.

- **Mediation and Conciliation**
  By nature of what we do, notably in our operations division, it is inevitable that we are drawn into situations of conflict between the complainant and the party complained against. Whilst the Ordinance does allow for penal measures, we have not generally resorted to them to resolve issues. Our greatest strength lies in our ability to deploy mediation skills to effect a satisfactory settlement between parties. Our view is that if we adopt an overly confrontational approach then this, over time, may negatively influence public perceptions e.g. the PCO is biased, tends to favour one party over another, or is inclined to overreact to what are genuine mistakes or relatively minor infractions of the law. In general, we have avoided recourse to the 'big stick' by offering a carrot. As I have implied, given the spectre of counter-terrorism

measures, it may well be that this is, unintentionally, the most realistic way in which to serve privacy interests in future. Simply, the 'stick' at our disposal has the prospect of becoming a much less formidable weapon.

- **Sustaining the Profile of Privacy**

  Much of what the PCO does is not only a matter of developing tenable policy positions. That is an important part of the picture but not the full picture. The full picture includes evaluating the ramifications of policy in terms of public image and goodwill. The PCO endeavours, via the 'products' it delivers to the community, to heighten public awareness, understanding and empathy. In short, we aim to exploit the full publicity value of policy in order to enhance the understanding of the public and keep privacy issues firmly on the front page.

- **Influencing the Public Mindset**

  There is little doubt that creating a culture that respects privacy is a massive challenge. Nonetheless, this task is central to the longer term success of the PCO and a key measure of its future performance. This vision is factored into everything the PCO does which places it in a race without a finishing line quite simply because the notion of a society in which there is absolute respect for privacy is fanciful. If the PCO were to achieve the unachievable it would become a redundant entity. That seems a long way off and in the meantime we have to address the reality of privacy, which is something quite different. The reality is that developing a culture that respects privacy is a painstaking and incremental process. There do not appear to be any quick fixes. However, we seek in what we do, notably our policies and strategies, to create a value that reflects a fundamental respect for the privacy of others. Conventional thinking regarding this superordinate goal dictates that the PCO alter public perceptions, attitudes and ultimately, behaviours. However, the psychology of attitudinal and behavioural change involves complex processes in which the outcome is by no means guaranteed. Only by unravelling those processes will we place ourselves in a position to build the culture we seek to establish. This line of reasoning gives rise to a principled belief that better research leads to better understanding, and the formulation of superior strategies with which to tackle identified problems. We are of the view that it is essential that our opinions and decisions are well informed because only through a closer understanding of what makes the community

'tick' will we be able to devise programmes that register with them, and result in the changes in behaviour we wish to promote.

11.4 So much for the tenets that guide the PCO. How do these translate in practice? The words consultation, education, communication and mediation have become something of an organisational mantra at the PCO in that they greatly influence the day-to-day practices of the office. Considerable value has been attached to these core concepts, and their implications for management style. I think that this emphasis is unlikely to change in the foreseeable future and that will lend an element of continuity to what we do. Good execution of these concepts will greatly help in the process of consensus building around personal data privacy in the community, which is a major outcome for the PCO.

11.5 I hope that in this paper I have done justice to the title and offered some thoughts on how the PCO works in an alliance with constituencies in the community to build awareness and compliance.

Our website contains a considerable amount of content and related links which may be of interest to those who wish to obtain a deeper understanding of the PCO and the way in which we strive to fulfil the objectives we establish for ourselves.

Raymond Tang
Privacy Commissioner for Personal Data

Office of the Privacy Commissioner for Personal Data
Suite 2401, 24th Floor, Office Tower
Convention Plaza
1 Harbour Road
Wanchai, Hong Kong

Tel: (852) 2827 2827
Fax: (852) 2877 7026
E-mail: pco@pco.org.hk
Internet: http://www.pco.org.hk

U:/kitty/S2070703.doc (26 June 2003)

Appendix I ~
Personal Data (Privacy) Ordinance

Data Protection Principles

PERSONAL DATA (PRIVACY) ORDINANCE
(Chapter 486)

SCHEDULE 1

DATA PROTECTION PRINCIPLES

1. Principle 1 - Purpose and Manner of Collection of Personal Data

(1) Personal data shall not be collected unless -
(a) the data are collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;
(b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and
(c) the data are adequate but not excessive in relation to that purpose.

(2) Personal data shall be collected by means which are
(a) lawful; and
(b) fair in the circumstances of the case.

(3) Where the person from whom personal data are or are to be collected is the data subject all practicable steps shall be taken to ensure that
(a) he is explicitly or implicitly informed, on or before collecting the data, of -
(i) whether it is obligatory or voluntary for him to supply the data; and
(ii)where it is obligatory for him to supply the data, the consequences for him if he fails to supply the data; and
(b) he is explicitly informed -
(i) on or before collecting the data, of -
(A) the purpose (in general or specific terms) for which the data are to be used; and
(B) the classes of persons to whom the data may be transferred; and
(ii) on or before first use of the data for the purpose for which they were collected, of -
(A) his rights to request access to and to request the correction of the data, and
(B) the name and address of the individual to whom any such request may be made,

unless to comply with the provisions of this subsection would be likely to prejudice the purpose for which the data were collected and that purpose is specified in Part VIII of this Ordinance as a purpose in relation to which personal data are exempt from the provisions of data protection principle 6.

2. Principle 2 - Accuracy and Duration of Retention of Personal Data

(1) All practicable steps shall be taken to ensure that -
(a) personal data are accurate having regard to the purpose (including any directly related purpose) for which the personal data are or are to be used
(b) where there are reasonable grounds for believing that personal data are inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used -

(i) the data are not used for that purpose unless and until those grounds cease to be applicable to the data, whether by the rectification of the data or otherwise, or
(ii) the data are erased

(c) where it is practicable in all the circumstances of the case to know that -

(i) personal data disclosed on or after the appointed day to a third party are materially inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used by the third party, and

(ii) that data were inaccurate at the time of such disclosure, that the third party-

(A) is informed that the data are inaccurate and

(B) is provided with such particulars as will enable the third party to rectify the data having regard to that purpose.

(2) Personal data shall not be kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data are or are to be used.

3. Principle 3 - Use of Personal Data

Personal data shall not, without the prescribed consent of the data subject, be used for any purpose other than -

(a) the purpose for which the data were to be used at the time of the collection of the data, or

(b) a purpose directly related to the purpose referred to in paragraph (a).

4. Principle 4 - Security of Personal Data

All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure or other use having particular regard to -

(a) the kind of data and the harm that could result if any of those things should occur;

(b) the physical location where the data are stored;

(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data are stored;

(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data, and

(e) any measures taken for ensuring the secure transmission of the data.

5. Principle 5 – Information to be Generally Available

All practicable steps shall be taken to ensure that a person can –

(a) ascertain a data user' s policies and practices in relation to personal data;

(b) be informed of the kind of personal data held by a data user;

(c) be informed of the main purposes for which personal data held by a data user are or are to be used.

6. Principle 6 - Access to Personal Data

A data subject shall be entitled to -

(a) ascertain whether a data user holds personal data of which he is the data subject;

(b) request access to personal data -

(i) within a reasonable time;

(ii) at a fee, if any, that is not excessive;

(iii) in a reasonable manner and

(iv) in a form that is intelligible;

(c) be given reasons if a request referred to in paragraph (b) is refused;

(d) object to a refusal referred to in paragraph (c);

(e) request the correction of personal data;

(f) be given reasons if a request referred to in paragraph (e) is refused; and

(g) object to a refusal referred to in paragraph (f).