Technological Ubiquity:
The Need for Consumer Privacy Protection

The Hong Kong Experience

Tony LAM, Acting Privacy Commissioner for Personal Data
Office of the Privacy Commissioner for Personal Data
Hong Kong SAR

Introduction

The marriage of computer and tele-communications technologies has created a new electronic networking environment on which business and services are delivered. Today, anyone who has a connection to the Internet is able to access easily an abundance of information that is made available online. No doubt, the technological advancement will eventually transform the way many organizations operate and virtually every aspect of our modern life.

The George Orwellian "Big Brother" metaphor has often been used to describe the relationship of a ubiquitous technology society surveying the activities of individuals by spying on chat rooms, newsgroups and forums. Industry experts observe that the ubiquitous network is going to be further highlighted by the emergence of new services enabled by wireless broadband access. The notion of Internet connectivity "any time", "anywhere" on "any device" is anticipated in the near future.

There is no absolute adversarial relationship between technological advances and the protection of consumer privacy. However, technology makes it all easy to collect, store and disseminate personal information. As more and more commerce and government services are delivered via the ubiquitous technology network, vast quantities of personal data about all of us will potentially be collected, stored and transmitted over the network. The past great protectors of data privacy: cost, distance, incompatibility, etc., are all disappearing in this ubiquitous network of technologies.

This paper examines the impact of technology on personal data privacy and provides a brief account of the Hong Kong's experience in implementing consumer data privacy protection.

Privacy

I would like to begin by saying that in Chinese society the concept of privacy is relatively new, in particular, privacy relating to personal data is a very new concept. 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.

Like many developed countries, Hong Kong faced obstacles in its pursuit of consumer privacy protection. In the early days, the importance of privacy was not a priority as government focused upon meeting the more basic needs of citizens, such as education and housing. More specifically arguments were voiced that business would become inefficient if privacy issues were allowed to get in the way. Others commented that privacy compliance would be expensive and result in the imposition of conditions that might create animosity in the community.

Impact on Privacy

The ubiquitous network of information and communications facilitates an affordable "cyber marketplace" for businesses and consumers in different parts of the world. Businesses see significant economies in operating in the new electronic environment that has global reach, with the prospects of cost reductions and enormous opportunities for growth. Similarly, for online consumers, the new environment offers infinitely expanded buyer information, competitive prices and a range of choices that are daunting to comprehend.

However, in spite of these apparent benefits, the advent of the information and technology age has also raised significant consumer protection issues. These issues represent new challenges to businesses, governments and consumers; and if not addressed, pose significant privacy risks and threats that may impact upon the trust and confidence among E-business participants.

The growing concern of potential privacy intrusion by advanced technology can be illustrated by the recent developments in wireless communications and RFID.

Wireless communications offer many benefits such as portability, flexibility and lower installation cost. The rapid development of wireless and mobile communications, coupled with the emergence of location-based devices, is creating a new wireless environment that offers the prospect of a wealth of services based on knowledge about the precise location of the user. An example is location-enabled emergency service such as vehicle theft tracking. However, location data, when used in conjunction with other information of a person, may ascertain the identity of the person and allow his or her where about to be tracked, any time and anywhere. While location data may offer consumers a public safety protection in emergency situations, they are concerned about the privacy implications of such data falling into the wrong hands.

RFID technology used in retail business such as RFID tags on garments brings significant advantages to business in cost reduction; assist them in better shelving and store layout to promote sales of popular items. Innocuous as it may seem, the technology does pose a threat of intrusiveness to customers' privacy. The RFID tag, when linked with personal information such as credit card payment data, can potentially be used to profile customers with tagged objects in respect of their shopping patterns. It is well known that RFID tags are highly durable and difficult to destroy, so unless customers are informed and/or have the choice to deactivate the function, then surveillance goes hand glove with the purchase of the tagged object.

It is reasonable to conclude that technological convergence and the ubiquity of information and communications have, on the one hand, brought considerable benefits in terms of product pricing and convenience. On the other hand it is equally clear that consumers see significant privacy risks in terms of the management of personal data by online data users. Not only are consumers concerned about sellers offering quality products and services, they are also concerned about their ability to exercise control over the use of their personal data.

Consumer Privacy Concerns

In today's E-business environment, concerns over privacy emerge when an individual is requested to provide personal data, for example, name, address, credit card number, etc. as part of an online transaction when he or she is dealing with a business partner over an open and unmanaged network such as the Internet. This occurs most obviously when individuals fill in online forms. In addition, there is often "unseen" collection of data, including data relating to the individual's online movements within and between web sites. The data collected from individuals may include sensitive information, such as credit card details and, if aggregated, can be used to track an individual's preferences and online activities. There is thus a risk that data could be intercepted during transmission and that they could be used or disclosed for unintended, unauthorized or fraudulent purposes.

The issue of privacy concerns more than just the security of personal data when the information is transmitted over open networks. It relates also to the collection, storage and use of the data, the right of the individual to determine when, how and to what extent others may share his or her personal information and the rights to request access to and correction of the data concerned. There is also a general lack of transparency about what personal data are collected and how the collected data will be used.

Privacy concerns are consistently reflected in consumer surveys conducted overseas and also in Hong Kong. A survey conducted in May 2003 by the IT practice group of a local firm (Stephenson, Wong & Co. http://www.Sw-hk.com) revealed that 83% of general Internet users feel that limited personal data protection restrains Hong Kong's E-business development. In the same survey, 86% of respondents felt that E-privacy, or security problems, would dissuade them from making payments online.

Our own public surveys 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. In our opinion survey conducted in 2004, 62% of the respondents (n=1051) expressed their concern of "misuse of personal data by third parties" when purchasing on the Internet. These findings provide a good illustration of a commonly held perception, rightly or wrongly, that there is a 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.

Addressing Privacy Concerns

The combined effect brought about by the ubiquitous society of technologies and the move towards a global economy has been to bring into sharp focus the fact that the protection of privacy has 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.

In 1994, the Hong Kong Law Reform Commission reviewed the status of privacy in other jurisdictions. This review indicated that there were three macro approaches towards institutionalizing the protection of privacy.

- Option 1 – Institute a statutory framework with the establishment of an independent regulatory body.
- Option 2 – Create a statutory tort of invasion of privacy to permit civil proceedings.
- Option 3 – Rely upon self-regulation, e.g. voluntary codes of practice and professional/ industry watchdogs.

Hong Kong adopted option 1 although the approach taken also embraces elements of option 2 and 3. The statute to protect privacy in relation to personal data is the Personal Data (Privacy) Ordinance. Compliance with the privacy law is promoted and enforced by the Office of the Privacy Commissioner for Personal Data ("the PCO"), which was established in August 1996. The statutory framework afforded by the privacy law ensures the independence of the PCO as a regulatory body, permits civil redress for any contravention of the provisions of the law, and empowers the Privacy Commissioner to promote self-regulation through issuing codes of practice and privacy guidelines.

The privacy law came into effect on 20 December 1996. The objective of the law is

obviously to protect the personal data privacy of individuals. It also serves an important purpose in contributing to Hong Kong's continued economic well being by safeguarding the free flow of personal data to Hong Kong from restriction by countries that already have data protection laws.

Our privacy law applies to both the public and private sectors and is based on internationally accepted data protection principles. It provides for statutory controls that address all the key privacy concerns arising from the use of electronic networks by individuals such as transparency, security, limitations on use/ disclosure, rights of access and correction and the right to opt-out from direct marketing approaches by data users. Accordingly, the PCO operates on the principle that "what is unlawful offline is unlawful online".

Hong Kong's Approach

The privacy law was novel to the business sector when it was introduced in Hong Kong. In the early stages of implementation the signals we were receiving had an apprehension about them. This apprehension was derived from established custom and practice around how we do business in Hong Kong i.e. a laissez-faire minimal interventionist economy.

We took notice of this apprehension because it was our belief, and remains so, that privacy law can only operate effectively if it is understood and accepted by business and the community more generally. A priority task was, therefore, to raise privacy awareness in the community at large in which personal data privacy was both understood and valued. We believed that this could only be achieved through a "cultural shift" in the collective consciousness of the Hong Kong community. In practice, it meant implementing changes in business practices that require a data user to notify individuals of its purposes of collecting data from them and to seek consent from the individual concerned for any different purposes of use.

It takes time to effect this "cultural shift" and we see our effort playing a significant role in facilitating the necessary changes. We regard continuous promotion as central to the creation of privacy awareness. In pursuit of our goal, we adopted a strategic approach that aims to:

- Promote a culture within the Hong Kong community that respects privacy.
- Enhance awareness of privacy protection through co-working arrangements with business, industry and professional bodies.
- Ensure privacy compliance through systemic improvements and a minimum of legal enforcement.
- Develop an environment that offers a balance between individual rights to privacy and other social, economic and public interests.

Policy on Good Privacy Practices

Today's practice of doing business focuses on strengthening customer relationship that is built on trust and confidence. Consumers are becoming more concerned, more informed, and more demanding with regard to the protection of their privacy. Adopting privacy protection practices makes good business sense as such practices can effectively address their concerns.

The legal framework of the privacy law provides the ground rules governing data privacy protection. Equally important though is the commitment of business and managers to ensuring compliance with these rules. This requires conscious effort from all parties concerned.

If this is accepted, then privacy protection has to be established as a core value that connects organizational culture with the best interests of consumers. The value can be viewed as an important indicator of business success and regarded by many as a way of differentiating competing providers. A commitment to creating this value means that all planning and implementation activities must be aligned with the vision of the future.

Though essential, creating the value may seem a rather obscure process. To make it more tangible it is necessary to encompass the value of good privacy practices into the business E-Privacy policy. This requires an organization to inform consumers of its commitment to the protection of their personal data, and honour the responsibility that commitment place upon management. The challenge then is for management to be able to "do what it says". Anything that is over-promised or under-delivered is likely to be counter- productive.

The E-Privacy policy implementation should be a process of deliberate and sustained improvement that requires constant compliance assessment and monitoring. It needs to operate in parallel with the conduct of a Privacy Impact Assessment ("PIA"). A PIA may be described as a systematic process that evaluates a proposed project initiative such as a strategic public policy or technology option in terms of their impact upon privacy. In this context, a PIA should seek to identify actual or potential privacy issues associated with the initiative and to examine the options available for mitigating any risks that have been identified. To be effective, a PIA needs to commence at the outset of the project planning rather than an afterthought. The outcome of any PIA should be measured against the influence it exerts upon proposals and strategic decision-making. Ultimately, the purpose is to ensure that decision-makers are cognizant of the privacy dimension and work towards decisions that are privacy enhancing.

The Hong Kong Experience

Questions have often been asked about the cost of compliance with privacy protection and what the pay-off of this investment is likely to be. One answer to that question is that, as some commentators have observed, it is not whether companies can afford to adopt good privacy practices, but rather a case of whether they can afford not to do so. Simply put, the choice is no choice. I do not disagree with this observation. However, I would add to this with a more positive review of the corporate pay-off from our business sector experience in Hong Kong:

- **Building trust and confidence.** Where management succeeds in guaranteeing the exactitude with which personal data is managed it is likely that this will have a corresponding effect upon the level of trust and confidence expressed by customers and other stakeholders. This can only be beneficial, especially in the world of online business transactions where privacy and security protocols assume special importance. Where the protection of personal data is demonstrated to be exemplary this will reflect upon corporate reputations and brand equity that could boost growth by reinforcing loyalty and expanding the customer base.

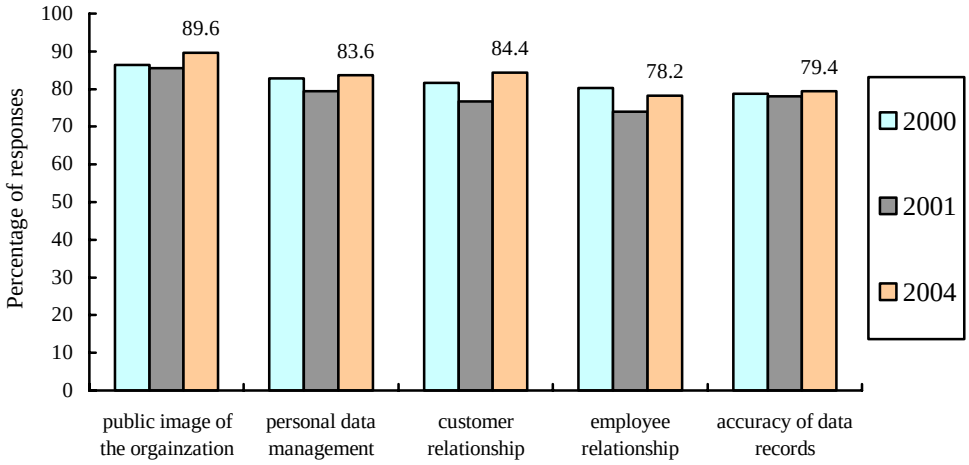
- **Gaining competitive advantage.** The logical extension to this benefit is that businesses should be able to use a high level of demonstrated trust and confidence as the basis for differentiating themselves from their rivals. Differentiation not only adds to the value of brands and their positioning but also offers business an alternative means of seeking competitive advantage.

- **Enhancing corporate governance.** Today's business environment demands complete, accurate, timely and relevant information to make informed business decisions. The most reliable source of information about a customer is the customer. With accurate information about their customers, businesses are able to effectively focus their efforts, time and resources to respond to customers' demands for personalized and customized services.

In Hong Kong, many business sectors and companies, particularly those in the information business such as banks, telecommunications and insurance companies, have realized the need to rise to the challenge and have voluntarily responded by introducing code of fair information practices or privacy policies. For them this was just part and parcel of being a good corporate citizen and a professionally run business that sought to accommodate new challenges rather than oppose them.

Each year, the PCO conducts an annual territory-wide opinion survey that maps public attitudes, and those of the business community, towards the implementation of the privacy law. Over the past years, our annual opinion surveys have shown, on the one hand, increased awareness in the community of privacy rights and, on the other hand, more and more business organizations recognizing the long term benefits that are to be derived from compliance with the privacy law.

The 2004 opinion survey showed that over 80% of the responses either agreed, or strongly agreed, that compliance with the law brought, and continues to bring, long term benefits to their business in terms of their public image, data management, and customer relation.



Conclusion

Since the establishment of the PCO in 1996, 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. In today's economic environment, the issue of privacy protection has often been portrayed as anti-business and privacy laws as restricting legitimate business activities. In Hong Kong, we have demonstrated that this is not the case.

As we all know, the individual right to privacy is not an absolute. Its protection, where relevant, has to be considered in the overall context of the collective rights of an enlightened society. Therefore our strategy in the Hong Kong was to approach the issues with patience, relying on understanding, communication, education, persuasion, conciliation, systemic improvements and a minimum of legal enforcement. In our implementation of the privacy law, we are proud to say that we have been instrumental in developing an environment that has made the "cultural shift" possible in our society. Our privacy legal framework is like a seedling. The fruits it bears, if any, depend very much on the environment that is cultivated around it.