Hong Kong Computer Society Innovation & Technology Series: Distinguished Speaker Luncheon

12:15 – 14:00 19 October 2010 (Tue)
The Soong Room, Dining Hall, Butterfield's
2/F, Dorset House, Taikoo Place

Good afternoon, ladies and gentlemen. Thank you for inviting me to talk about the challenge of personal data protection.

When Stephen asked me to attend this luncheon, he said I can talk anything I like about personal data protection. At this juncture, I think it is most opportune for me to talk about the Octopus episode. We have just published the investigation report yesterday giving details of our findings and recommendations. I won't bore you with the details here. Suffice it for me to say that this is an important lesson for Hong Kong, for me as the Privacy Commissioner, the business community and the man on the street. I'll coin it as a major milestone in the history of personal data privacy protection.

Protection of personal data privacy as a basic human right is still a relatively new area. It probably did not exist as a stand-alone concept decades ago. I still remember a real experience of personal data privacy I had when I started my career in the Post Office as a junior manager. I was in charge of mail delivery and read on a daily basis letters written by my subordinates.

One of them was a Post Office veteran approaching his retirement age. He received a letter seeking our help to disclose the new address of someone who had recently moved. We did keep records of this kind for mail redirection purposes and he, being a kind-hearted and helpful person, readily complied with the customer's request. When I asked if he had obtained the authority of the person concerned, he was dumbfounded. Obviously, the need to respect and protect privacy in respect of personal data never crossed his mind.

Ladies and gentlemen, this was a true incident that took place more than three decades ago.

Incidentally, at that time the word "computer" probably also did not exist. Computing in those days was called electronic data processing. Well, times have changed. Computer skills are now learnt at primary schools. The Office of the Commissioner for Personal Data was set up some 14 years ago to educate the general public and to take enforcement action as necessary as regards compliance with the requirements under the Personal Data (Privacy) Ordinance. Thanks to the efforts of Stephen and other predecessors of mine, businesses and individuals in Hong Kong are now generally aware of the rights and obligations to protect personal data privacy.

The Octopus incident is unique in that the handling of personal data of more than two million people in Hong Kong is involved. Thanks to the media and the hue and cry of different interest groups, the recent Octopus incident has brought the awareness level to an

all-time high.

I noticed that there was a breakthrough in this year's Miss Hong Kong Beauty Contest. Perhaps for the first time in the history of the Beauty Contest, questions were asked from the contestants on the subject of personal data privacy. To achieve this quantum leap in privacy sensitivity level, my Office must have saved countless man-hours and millions of dollars in advertising and promotion.

People say that the Octopus incident is just the tip of an iceberg. Very true. This is because the malpractices identified in the Octopus case have been pretty widely adopted in the business world, namely,

(1) Excessive collection of customers' personal data, an indication of a general lack of due regard to privacy. In the Octopus case, the Hong Kong Identity Card numbers were collected for the purpose of customer authentication when in fact other data they have collected already, such as telephone numbers and home addresses, would have served the same purpose adequately.

    I am sure you will be able to recall immediately many instances in your daily life when you wondered why your Hong Kong Identity Card number or copy of your Hong Kong Identity Card were sought by the other party in a business transaction when there were obvious substitutes. When you have the same encounter next time, re-think before complying with the request, and quoting as necessary the famous Octopus case.

(2) The second malpractice was that the Personal Information Collection Statement was poorly laid out and presented. The Statement was meant to inform the customers of the purpose of the use of the personal data collected, and the classes of persons that the data would be transferred.

In the event, the font size used for the statement was about 1mm x 1mm for English and 2mm x 2mm for Chinese, so small that people with normal eyesight would find the words difficult to read unless aided by a magnifying glass.

Further, the purpose of use of personal data and class of data transferees were couched in such liberal and vague terms that it would not be practicable for customers to ascertain with a reasonable degree of certainty how their personal data could be used and who could have the use of them.

Again, I am sure you have many similar experiences. Indeed, it is not uncommon to find in our daily business transactions that the purpose of use of personal data is defined as ***"such purposes as the Company may from time to time prescribe",*** and that class of data transferees was defined as ***"selected companies which will provide information of services in which customers may be interested"*** or ***"all business partners"*** etc. In the circumstances, our personal data are entirely at the disposal of the companies collecting the data. This is grossly unfair.

(3) The third malpractice concerned cross-marketing whereby a company transfers its customers' personal data to a partner company for marketing the latter's products and services. The transferor company simply selects the required customer data and plays little or no part in the marketing process but receives monetary gains from the partner company as a reward for the data transfer. The transaction in essence is sale of personal data.

Although the sale of personal data by a data user is not prohibited by the Ordinance, it would not normally be regarded as the original purpose of data collection or as a directly related purpose. For example, when a customer applies for a credit card from a Bank and supplies his personal data, he would only expect the Bank or the Bank's group companies to approach him for marketing related products and services of direct interest to him.

These activities serve to enhance customer loyalty and are common in a competitive business environment like Hong Kong. It would fall outside his reasonable expectation that the data would be transferred or shared with a third party for monetary gains. In the circumstances, consent from the customer has to be sought.

More often than not, the customer is only provided with one space on the credit card application form to sign and he has to choose between (i) giving up the application for the credit card

and (ii) giving his "bundled consent" agreeing to the terms and conditions for the credit card service as well as sale of his personal data by the Bank when in fact he finds the sale of his personal data objectionable. Such "bundled consent" is not true consent. True consent should be express and voluntary, indicated by a separate signature or by ticking a box.

(4) The fourth malpractice has got to do with cross-marketing also. Under an arrangement between the transferor company and its partner company, the partner company would promote its products and services by calling the customers of the transferor company and in the name of the transferor company. Such arrangement would affect the customers' right to object in a timely fashion to the data transfer and the further collection of their personal data by the partner company during the sales call. In effect, the customers have been deceived as regards the identity of the caller.

Ladies and gentlemen, you may be wondering why these malpractices have been so common. Your guess is as good as mine. My work career has been very much service-oriented and I have been working with many reputable service organizations in Hong Kong to promote customer service excellence and to champion corporate social responsibility.

With this background, I must say that I was appalled to find that these same organizations are by no means customer-centric in the

areas of personal data privacy. Lawyers and compliance auditors from these organizations have been arguing with me in the past two months or so defending their positions.

The conclusion I can draw is that for an organization to be truly customer-centric, a total organization-wide approach has to be adopted, involving not just the customer service professionals but all members of the organization, including the lawyers and the compliance auditors. In particular, a top-down approach with leadership from the top is essential.

In the past, I do not believe privacy issues attracted the attention of corporate CEOs. They would have difficulty in finding a place in the agenda of Boardroom discussion. There are just too many other priorities that seemed more important.

I now suggest that the Octopus incident is a wake-up call to the top management of corporations. Just look at what happened to Octopus. People placed great trust on this household name and expected from the Octopus management nothing less than good governance and a high respect for human rights, including personal data privacy. The malpractices I just referred to have jeopardized their credibility and damaged their reputation disproportionately.

I would appeal to all CEOs that they must accord to personal data protection the priority that it deserves. The Octopus incident is a turning point. With the heightened sensitivity of the customers over

personal data protection after the Octopus incident, CEOs would henceforth find customers more vocal and assertive in this human rights area.

A paradigm shift is called for and new thinking on their part is required. My proposition is that respect for personal data privacy has to be integrated into the business processes and operational procedures throughout the organization in order to achieve enduring and higher level of success for the organization. Organizations should embrace personal data privacy protection as part of their corporate culture.

Ladies and gentlemen, I know most if not all of you are from the IT industry. I suggest to you to manage your IT projects in future with a Privacy by Design approach, if you are not already doing so.

Privacy by design is an approach that treats personal data protection as an integral part of any project or system that involves personal data. The idea of *privacy by design* is that personal data protection is not a silo process and therefore must be fully integrated in the life-cycle of any project or initiative from planning to execution.

During the planning stage, *privacy impact assessment* should be carried out to identify any potential issue that a project or initiative may have on personal data and privacy protection and how they may be avoided or mitigated prior to any actual design.

Even the final design has taken care of all the issues identified in the *privacy impact assessment*, given the changing nature of the business environment, regular *privacy compliance assessments* should be carried out throughout the lifetime of the project to ensure continuous compliance with the *data protection principles*.

Apart from the Octopus case, I would like to quote two recent cases to illustrate the concept of Privacy by Design. They are all IT-related.

The first case related to the use of fingerprint recognition system. A while back there was a case on the use of fingerprint to record employee attendance in a furniture company. While it provided a convenient and perhaps speedy solution to a mundane task, the use of sensitive biometric personal data for the purpose of attendance recording was too privacy-intrusive a measure.

Furthermore, the internal rules of the company provided for immediate dismissal for those employees who did not use the fingerprint system. The disparity in bargaining power between the employer and the employee meant a fair consent could never had been given by the employees in the circumstances. A *privacy impact assessment* would have picked up these potential controversies before the scheme had the chance to take off.

The second example I'd like to mention isn't so much a fault at the design stage, but at its execution. Google admitted that it had

inadvertently collected Wi-Fi payload data while snapping pictures for the Street View project. It was revealed later that the intention was only to collect Wi-Fi station names and not the payload data.

The project manager, while selecting the software, overlooked the fact that the software was also capable of capturing the payload data. Such an execution error would not have been detected in a *privacy impact assessment* but should have been picked up in a subsequent *privacy compliance assessment.*

I recommend adopting a *privacy by design* approach because it leads to a personal data protection regime that is proactive and not reactive, preventive and not remedial, by default and not as an optional extra, and also end-to-end and not piecemeal.

Above all else, a Privacy by Design approach has to be truly customer-centric. The whole idea is to have the interests of the customers in your mind and in your heart, and not just doing the least possible to meet minimum legal requirements, and focus on how to defend you position when challenged in the grey areas.

At this juncture, ladies and gentlemen, I would also like to challenge the commonly-held belief or misconception that personal data protection is a trade-off against business functions or innovation. I am talking about the common belief that if you want higher protection on personal data, you will have to sacrifice functionality or innovation.

This notion is probably true if you are trying to retro-fit personal data protection to systems that is already in operation. Not only will it cost more to bolt on privacy protection compared with designing it as an integral part of the system from day one, sometimes it is downright impossible to do so and that's when the sacrifice of functionality comes in.

All in all, it pays to invest on personal data protection at the earliest possible time as the cost of recovering from the adverse publicity on personal data protection on an organisation or its management would be far more than the cost of building a proper protection system from ground up. In this regards, the Octopus incident is a lesson for everyone.

As I pointed out earlier, attaining true customer centricity and sustainable business success requires a fundamental enterprise-wide shift in thinking and reorientation of enterprise's value proposition. You have to recognize that a good personal data protection system in place offers you a unique competitive advantage among your peers.

Today's business competition is no longer concerned with just price and service quality. You have to compete in new areas like environmental friendliness, corporate social responsibility and protection of human rights. An enterprise which cares about personal data privacy would inspire consumer confidence. Customers may be more inclined to volunteer optional information you seek from

them. You will avoid collecting fictitious information which happens when the customers want your service but are wary of your company's level of privacy protection.

Ladies and gentlemen, I hope I have made out a convincing case for greater privacy protection. If there is just one thing you would like as a take-away for this luncheon, remember the catchphrase: Privacy by Design. On this note, I would like to end my talk. Thank you very much for your time.