Speech delivered by Mr. Allan Chiang,
Privacy Commissioner for Personal Data (Hong Kong)
at Privacy Laws & Business 24th Annual International Conference
on 13 July 2011, St. John's College, Cambridge, United Kingdom

Data Protection: Recent trends and developments in Hong Kong

Ladies and Gentlemen,

Data Breach in Recent Years

As you are probably aware, among the jurisdictions in the Asia-Pacific region, Hong Kong is one of the few which have dedicated legislation on personal data protection for over a decade.

But, despite the promotional efforts of my Office, privacy rights over personal data had never been a hot topic in Hong Kong until recent years when we witnessed a series of privacy catastrophes gaining widespread media attention.

In 2006, we probed into a serious data leakage incident which involved disclosure on the internet of 20,000 people who had lodged complaints with the Independent Police Complaints Council against the Police.

After that, more incidents of data leakage or loss broke out, involving large quantities of personal data held by major data users, including government departments and universities. The situation worsened and culminated in the loss of 16,000 patient records in 2008 in public hospitals.

This trend continued. From mid-2008 to late 2009, classified and sensitive documents containing personal data held by the Immigration, Fire and Police Departments were leaked on the internet through the file-sharing software: "Foxy".

The incidents have alarmed the community and highlighted the need for responsible privacy practices in managing personal data.

Unauthorized Use of Customers' Personal Data

In parallel with these data leakage incidents, complaints about business misuse of customers' personal data have grown.

They underlined a widespread malpractice adopted by many banks and some other big corporations with a large customer database whereby customers' data are transferred to third parties for direct marketing purposes, without explicitly and specifically informing the customers of the purpose of the transfer and the identity of the third parties, or seeking their consent.

In turn, this had generated direct marketing approaches to people for unsolicited products and services. Telemarketing calls, in particular, have caused a great nuisance to the community. It is not uncommon for the man in the street to receive several telemarketing calls a day.

The extreme persuasiveness of these junk calls is probably a unique Hong Kong phenomenon for two reasons. First, the household fixed line and mobile subscriber penetration rates in Hong Kong are among the highest in the world, around 100% and 200% respectively. Secondly, telephone services in Hong Kong are very cheap. Rental for fixed lines and subscription fees for mobiles are charged for less than GBP10 per month and there is no charge for individual calls.

The Octopus Incident

This offensive telemarketing approach confronted a serious challenge when a landmark privacy intrusion event broke out in mid-2010. It concerned the misuse of customer data held by a group of companies which operate an extensive smartcard payment system called Octopus.

The Octopus card is the equivalent of the Oyster card in this country except that the scale is much larger in terms of the number of service providers and card readers. It is more widely used than just paying fares for public transport. It almost obviates the need for change in the daily lives of the Hong Kong people.

Octopus's majority shareholder is the Mass Transit Railway Corporation or MTR, the equivalent of the London tube in this country. In turn, the majority shareholder of MTR is the Hong Kong Government.

Octopus operated a customer reward programme whereby registered members could earn Reward Dollars for making purchases from Octopus' business partners by presenting the Octopus card. The Reward Dollars earned may be redeemed for goods and services from the business partners.

Since March 2010, subscribers for the programme started to complain about Octopus' transfer of their personal data to third parties for direct marketing purposes without their knowledge or consent.

We investigated into the complaints and found, among other things, the following contraventions:-

First, the notice informing the customers of the purpose of the use of the personal data collected, and the classes of persons to whom the data would be transferred, was poorly laid out and presented. For example, the font size used for the notice was so small (about 1mm x 1mm for English) that people with normal eyesight would find the words difficult to read unless aided by a magnifying glass.

Secondly, the purpose of use of personal data and classes of data transferees were couched in liberal and vague terms. 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.

Thirdly, Octopus had, without the customers' explicit consent, transferred their personal data to a number of partner companies for marketing the latter's products and services. Octopus played little or no part in the marketing process. But it received monetary gains from the partner companies as a reward for the data transfer. The transaction in essence was sale of personal data.

Finally, under prior agreement with Octopus, one partner company promoted its products and services by calling Octopus' customers in the name of Octopus. In effect, the customers have been deceived as regards the identity of the caller.

The Octopus incident had attracted prolonged media attention and the hue and cry of different interest groups in Hong Kong. It was rated as one of the top ten news stories of 2010 by many newspapers in Hong Kong.

I coined it a major milestone in the history of personal data protection in Hong Kong, characterized by a number of unique features:-

(1) It represented the tip of an iceberg as similar misuse of customers' personal data was widely adopted by business enterprises such as banks with a large customer database.

(2) It involved the handling of personal data of 2.4 million people, one-third of the entire population of Hong Kong, and substantial monetary gains.

(3) Octopus is a household name which all Hong Kong citizens have a high regard for. When they found out that their personal data had been traded as commodities for the private gains of Octopus, it was no surprise that they reacted with a sense of betrayal and anger.

(4) As I explained at the outset, the ownership of Octopus can be traced to the Government. Hence the incident generated immense political interests and fuelled vicious attacks against the Government for maladministration.

Effects on Octopus

The effects on Octopus for its outright failure to observe privacy and data protection were detrimental. The loss of public trust and damage to its corporate image are probably irreparable. The public outcry did not subside until it had taken a series of drastic remedial actions as follows:-
(1) It accepted all my recommendations and those of other regulators as regards enhancing personal data protection.

(2) It donated to charity all the revenue generated by its data transfer to third parties, viz. HK$57.9 m.

(3) It pledged that it would focus its core business on providing smart card services to customers and it would no longer participate in activities that require the provision of customer data to merchant partners for marketing purposes.

(4) Its CEO and Board chairman resigned and retired respectively (the latter purportedly as part of a natural succession plan).

The incident has more far-reaching consequences.

Impact on the General Public

It is perhaps no exaggeration to say that Octopus provided a human rights lesson for the Hong Kong community. It has brought public awareness and understanding of their privacy rights over personal data to an unprecedentedly high level. Media reports on privacy and data protection issues are more prevalent than ever before.

In a survey conducted by an internet security company earlier this year, it was found that 85% of Hong Kong people surveyed were extremely or very concerned about misuse of their personal data.

Impact on the Office of the Privacy Commissioner for Personal Data

As you can imagine, the workload of my office has also been affected. At its peak, the number of complaints received has increased by 44% compared with a year ago. The public is not just aware of their privacy rights and is more vocal than before.

On the positive side, my office must have saved countless man-hours and millions of advertising and promotion dollars in raising public awareness of data protection and encouraging compliance with the privacy law.
Indeed the demand for general education from the public, and advice and assistance from organizational data users has been overwhelming. In

response, we increased by some 80% the number of seminars and workshops we offered to the public and to the executives. We also issued a Guidance Note on the collection and use of personal data in direct marketing.

We have also been playing an active role in incorporating privacy and personal data protection into the liberal studies curriculum of secondary schools and relevant degree programmes of universities.

In a way, the Octopus incident could not have happened at a better time from our perspective because it coincided with the Government's public consultation exercise to review and amend the legislation on personal data protection to ensure it is still adequate and relevant.

In the consultation process, we have been championing a great number of initiatives to enhance data protection. These include acquisition of the power to impose monetary penalty for serious privacy contraventions and to award compensation to aggrieved data subjects. We expected to win support from the public and the legislature as they expressed disappointment at our lack of such sanctions against Octopus for its privacy contraventions.

I should add that the Octopus incident has provided two major learning points for us.

First, we have learnt to strengthen our regulatory power by partnering with other regulators, leveraging their legislative mandates, institutional tools and enforcement powers.

As I mentioned earlier, the unauthorized transfer of customers' personal data to third parties for direct marketing for monetary gains were not uncommon in Hong Kong. The trades involved included the banks, the telecommunication operators and the insurance industries. Like us, the corresponding regulators for these trades were under great pressure to address the problems. They acted swiftly and forcefully in order to dampen the public outcry.

They issued instructions and reminders to the enterprises concerned to

ensure that they comply with the law and my guidance. The Hong Kong Monetary Authority, which oversees the banks, went as far as to direct the banks to suspend the transfer of personal data to unrelated third parties for marketing purposes unless and until they were able to confirm full compliance with the law and the Guidance Note I issued.

Secondly, many enterprises have realized that the reputation risks associated with privacy contraventions are so high that they can ill afford to ignore privacy issues in their corporate governance. Capitalising on this heightened sensitivity for data protection, I have commenced last month a policy of naming and shaming.

When we publish a report after formal investigations on public interest grounds, we will invariably name the organizational data user which has contravened the legal requirements. This practice should invoke the sanction and discipline of public scrutiny and generate an enhanced deterrent effect.

The Government Reaction

As I mentioned earlier, the Octopus incident was very much politicized. One legislator went as far as to propose in the Legislative Council (the equivalent of the Parliament in this country) the setting up of a select committee to review the transfer and sale of customers' personal data in the whole commercial sector.

To allay the public outcry, the Government introduced, as part of the consultation exercise for the legislative reform, new proposals to address specifically the data breach issues highlighted in the Octopus incident. These include:-

(1) introduction of additional specific requirements on the collection and use of personal data for direct marketing purposes, and to make it an offence if a data user does not comply with the requirements and subsequently uses the personal data for direct marketing:-

- requiring the data user's notice to the data subject about data collection to be reasonably specific about the intended marketing

activities, the classes of persons to whom the data may be transferred and the kinds of data to be transferred;

- the presentation of the information should be understandable and reasonably readable; and
- the data subject should be provided with an opportunity to opt out from the intended use of his/her personal data.

The offence attracts a fine of HK$500,000 and imprisonment for three years.

(2) making unauthorized sale of personal data by data user an offence, punishable by a fine of HK$1,000,000 and imprisonment for five years;

(3) generally raising the penalty for contravention of the legislative requirements;

(4) empowering my office to provide legal assistance to an aggrieved data subject who intends to institute legal proceedings against a data user to seek compensation.

In sum, it appears there was a community consensus to tighten up control over the collection and use of personal data. But is this a passing fad or an enduring trend that will underwrite a new era of better corporate performance embracing data protection?

Ladies and gentlemen, draw your own conclusion based on the events that unfold themselves thereafter, as I will now describe.

The Business Sector Response

First, there are signs that the Octopus case has served as a wake-up call to those enterprises which had neglected the issue of personal data privacy in the past.

For example, we have launched a new series of professional compliance workshops tailored to the needs of executives dealing with personal data in different work contexts. 25 such workshops were organized in a matter of 3 months from April to June 2011 and the seats were sold like hot

cakes. The initiative has the support of 25 leading professional organizations, trade associations and chambers of commerce: an indication of the recognition in the corporate world that personal data protection is vital to good corporate governance and business success.

Since issue of the investigation report on Octopus and the Guidance Note on collection and use of personal data in direct marketing, I have been invited to speak on privacy and data protection on numerous occasions. I have witnessed that this subject has finally received top management attention and that attempts are being made to incorporate privacy considerations into business processes and management practices.

For example, a review of the credit card application forms provided by the banks two months ago revealed that that their notices to customers as regards collection and use of personal data have generally followed our Guidance Note.

More recently, I have found to my pleasant surprise that a reputable social service group in Hong Kong has published a corporate social responsibility guide for the small and medium enterprises and there is coverage on privacy and data protection.

However, all that glitters is not gold.

That customers' personal data are to be exploited for the benefit of enterprises at the expense of customers is a deep-rooted notion that cannot easily be swayed.

Only three months ago, a Hong Kong-based multi-national company advertised in the press an opening bearing the title: "Data Exploitation Analyst". It pretty much sums up the mainstream thinking of many corporate executives in Hong Kong.

Going back to the banks' credit card application forms, I hasten to add that we simply found them generally meeting the legal requirements in the collection and use of customers' data for direct marketing. I am actually disappointed that they are less forthcoming in following the good privacy practices recommended in my Guidance Note.

Specifically, the Guidance Note advises enterprises to design their service application form in a manner that does not bundle, on the one hand, the customer's agreement to the terms and conditions for the provision of the service with, on the other hand, the customer's consent to the use of his personal data for marketing any products or services not related directly to the services he seeks. We recommend inviting the customer to "tick" a box or giving a separate signature specifying whether the customer agrees to such unexpected use of his data, including sale of personal data. However, most of the banks do not provide this opt-out facility in the service application form. Apparently, they prefer to continue to exploit customers' personal data and ignore the customers' right of self-determination over their personal data.

Much to my regret, I also note that the Government's most recent proposals to implement legislative amendments are beset with crucial flaws.

For example, as regards sale of personal data by the data user for a monetary gain or in kind gains, the Government permits the data user to inform the data subject any time *after* collecting the data that the data are to be sold. This is out of keeping with the present legislation which requires the purpose of use of the data to be made known to the data subject *on or before* collecting the data. With this delay approach, the data user's notification that the data would be sold can take place at any un-predetermined time after data collection. Worse still, it would be incumbent on the data subject to make a specific opt-out request in response to the notification. If the data subject does not respond within 30 days, he would be deemed to have *not* opted out and the data user may proceed to sell the data to third parties. This deeming rule in effect legalizes what would not be permissible under present legislation, that is, sale of personal data by data users without the explicit consent of the data subject. It represents a retrograde step in enhancing data protection.

Further, the Government has decided not to pursue the proposals to strengthen the sanctioning power of my office to include award of compensation to aggrieved data subjects and imposition of a monetary penalty for serious contraventions of Data Protection Principles.

Setbacks looming up?

Shortly after publication of my investigation report when the Hong Kong public points the finger of scorn at Octopus, I thought the notions of respect for privacy and data protection must have, once and for all, deeply ingrained in their minds.

Due to two recent events, I now have second thoughts.

The first event was connected with the hacking of Sony's PlayStation Network in mid-April 2011, which resulted in a major data leakage and a suspension of its services worldwide. In view of the seriousness of the matter, I entered into a dialogue with Sony's top management demanding that their services should only be resumed after adequate and appropriate remedial measures had been taken. Somehow it took Sony up to early June 2011 to give assurance to that effect and resume service.

In the event, Hong Kong happened to be the last 3 places of Sony's service resumption. Nobody in Hong Kong has congratulated me for being tough and acting in his/her data protection interest. Instead, I received a number of complaints from the public about why Sony's services could not have been restored earlier so that they can jump back to the online games again.

The second event is related to the Government's unprecedented scheme this year to provide a cash handout of $6,000 to every Hong Kong resident.

The scheme requires all beneficiaries to register but there are suggestions that the Government should make use of its existing payment systems.

In particular, if the existing Government systems for disbursing social security and social welfare payments were used, it would save the trouble of registration by the recipients, many of whom are elderly and physically challenged people.

The Government did not accept the suggestions on grounds of data

protection. The use of existing payment systems involves the use of personal data previously collected from the payment recipients such as bank account details. Such use of personal data, unless agreed by the recipients, is not permissible as, according to the Government, the purpose of the one-off cash handout scheme is different and not directly related to the original purpose of collection of the data, which is provision of social welfare.

These Data Protection Principles, however, were played down or even sneered at by some critics. They argued that the privacy law was too rigid and posed an unnecessary burden to the under-privileged.

Obviously, these arguments would find favour in the eyes of some sectors of the community. But they are wholly misconceived as they run contrary to the rule of the law, which is highly treasured as one of the cornerstones of Hong Kong's way of life.

The lesson for me is that there is still a long way to go for me to champion privacy and data protection in Hong Kong. But I know I am not fighting a lonely uphill battle.

Ladies and gentlemen, I am here to share my problems with you and to benefit from your wisdom and experience. In the past 3 days I have gained a lot listening to and interacting with you and I look forward to more and continued sharing with you through other channels after the conference.

Thank you.