Keynote Address delivered by Mr. Allan Chiang,
Privacy Commissioner for Personal Data of Hong Kong
at Symposium on Personal Data and Privacy Protection:
A Comparative Perspective
on 10 February 2012
Council Chamber, University of Hong Kong

Personal Data Protection through Creativity and Partnership

The Watershed in 2010

As you can figure out from my CV, I am pretty new to my job. I started off in August 2010, some 18 months ago, when, using the words of Charles Dickens, it was the best of times and the worst of times.

It was definitely a critical time because we were in the course of an investigation into a landmark privacy intrusion case, namely, the Octopus Rewards programme which involved 2.4 million people in Hong Kong. As it turned out, we concluded that Octopus was at fault for the transfer of its customers' personal data to a number of partner companies for marketing the latter's products and services without the customers' explicit consent. The case has far-reaching consequences. Notably, it raised public awareness and understanding of individuals' privacy rights concerning personal data to an unprecedentedly high level.

At the same time, heightened public and media sensitivity and scrutiny posed immediate challenges to us in a number of ways. First, we have faced a drastic increase in the demand for our services. Statistics show that the number of complaints on personal data privacy intrusion in 2010 increased by 18% compared with 2009. This figure increased by a further 26% in 2011.

The Constraints

To tackle the workload problem, I asked for additional resources from the Government and succeeded, but only to a limited extent. As you can

imagine, the extra funding allocated to us has not been commensurate with the increase in workload.

Even more challenging is the fact that public expectation has been built up that we should be more vigilant in monitoring compliance and more rigorous in taking enforcement action. This is well recognized by the Government which has spearheaded the review of the Personal Data (Privacy) Ordinance. The formal public consultation on a number of proposed legislative amendments was completed by the end of 2010 and the Bill is now being discussed at the Bills Committee of the Legislative Council.

I note with much gratification that the Bill contains provisions which specifically address the grave public concern brought up by the Octopus case, namely, the need for an enterprise to give its customers an informed choice before collecting and using their personal data for direct marketing purposes or an outright sale to third parties. The new regime envisages much tightened control through a combination of procedural safeguards and sanctions. The maximum penalty for an offence is a fine of $1m and imprisonment of 5 years.

Admittedly, these measures are tough but please note that the scope of application is restricted to direct marketing or related activities only. Further, the complainants of these offences will have to rely on the Police and the Director of Public Prosecution to take their cases forward. My duty remains to make referrals only.

However, many members of the public who come to my office to lodge complaints on privacy intrusion have a much higher expectation of my enforcement power under the Bill. I believe they will expect a significant strengthening of my sanctioning power to address their grievances. Indeed, we have been very vocal in expressing the need for my office to undertake the criminal investigation and prosecution of data protection cases. But these proposals have been shelved by the Government. We also failed to secure the Government's endorsement to empower us to impose monetary penalties for serious privacy contraventions and to award compensation to aggrieved data subjects, despite the aspirations

expressed by many sectors of the community in response to the Octopus incident.

Positive Thinking brings Creativity and Partnership

I have probably portrayed a gloomy aftermath of the Octopus incident and suggested that my job is mission impossible. This is not my intention. As a positive thinker, I tend to confront constraints rather than surrender to them. I would like to share with you what can be achieved through creativity and partnership.

Privacy is more than a Legal and Compliance Issue

First and foremost, I raise the bar by treating privacy and data protection as more than simply a legal and compliance issue.

In day to day work, we are always confronted with legal challenges that the matter in dispute falls outside our jurisdiction and therefore we should not make any interference. For example, you will remember that the Octopus management had insisted that they have not done anything legally wrong, which we disagreed. But they did apologize to the public that they could have been more sensitive to public sentiment concerning privacy, and could have handled the matter better.

Similarly, in the initial phase of our inquiries with Google on the wrongful collection of Wi-Fi payload data by its Street View car in 2010, it responded with a query as to whether the Wi-Fi payload data is "personal data" under the purview of the Ordinance.

More recently in mid-2011, when we looked into the hacking of Sony's PlayStation Network which involved data breach of some 400,000 Hong Kong accounts, we were greeted with challenges from legal professionals as to whether I was empowered under the Ordinance to investigate into the matter.

Our response to these challenges was simple. We asked these companies to reflect if it really made business sense to them to simply leave the issue in the hands of their legal and compliance professionals. Invariably they

came to realize that the reputational risk associated with the privacy contraventions was so high that they should not be satisfied to do the least possible to meet what they thought was the minimum legal requirements, and focused on how to defend their position when challenged in the grey areas. In the end, we secured the co-operation of their top management in addressing the real issues and rectifying the mistakes.

Indeed, one key message to the business community in my speaking engagements in the past 18 months has been that enterprises should, as part of their corporate social responsibilities, incorporate privacy into their business processes in much the same way that other core values such as fairness, transparency and proportionality, are. I have been trying to impress upon them that today's business competition is no longer concerned with just price and service quality. To achieve enduring and higher level of success, organizations have to compete in new areas like environmental friendliness and protection of human rights. They should embrace personal data protection as a business imperative to earn and maintain customer trust and confidence.

Unleash the Full Potential of Existing Legislative Empowerment

I hasten to add that even under the Personal Data (Privacy) Ordinance as it now stands, I have found that there is plenty of room for me to do more.

For example, one of my statutory duties is to promote awareness and understanding of, and compliance with, the provisions of the Ordinance. To this end, the sky is the limit. I believe prevention is better than cure. Hence education and promotion targeted at corporate data users can be equally if not more effective than enforcement against contraventions. It is an area to which devotion of more resources is definitely rewarding.

Guidance to assist Compliance

In parallel with my public release of the investigation report on the Octopus incident, I issued a Guidance Note on the Collection and Use of Personal Data in Direct Marketing. This has proved to be extremely useful to marketing professionals as it provides comprehensively practical

advice on compliance with the law based on our enforcement experiences and developments in the interpretations of the law.

Before 2010, we have only 3 fact sheets and 3 guidance notes that provide corporate data-users guidance on compliance with the law in various subject areas. As at today, the number of guidance notes has grown to 10. They cover direct marketing, mobile service operation, electioneering, property management, fingerprint collection, data breach notification, CCTV surveillance, Internet services, use of portable storage devices and personal data erasure and anonymisation.

I have also embarked on the initiative of running professional workshops on data protection tailored to the needs of executives dealing with personal data in different work contexts. They cover the subject areas of marketing, property management, human resource management, I.T. management, handling data access request, banking operations, financial services and insurances.

This compliance workshop series is the first of its kind in Hong Kong. From April 2011 to the end of last month, 55 such workshops were held. I have been capitalizing on the wake-up call effect that the Octopus incident must have on the senior management in the corporate world. I believe that many of them who might have previously overlooked privacy and data protection must have awakened to its importance in good corporate governance and business success.

Indeed, the initiative has the support of 26 leading professional organizations, trade associations and chambers of commerce. I have not spent a single cent on marketing or promoting the workshops. I simply rely on the efforts of these supporting organizations to inform their members of the timetable and contents of the workshops. Partnership really helps. All workshops held were over-subscribed.

Industry-specific Promotion Campaign

As a further example of how closely we partner with corporate data users, I should point out that every year we partner with one industry to promote privacy and data protection among its members. We used to partner with

those industries which attract the most privacy complaints. Past partners were the Hospital Authority and the Federation of Insurers. This year, we are partnering with the Communication Association of Hong Kong which covers the business sectors related to the information communications technology.

Publication of Investigation Report to promote Compliance

It is perhaps no exaggeration to say that the Octopus incident was a landmark case in the history of data protection in Hong Kong. For various reasons, it attracted exceptionally prolonged media attention and the hue and cry of different interest groups in Hong Kong. Indeed, it was rated as one of the top ten news stories of 2010 by many newspapers in Hong Kong.

The power of the media demonstrated in this case has prompted me to make more frequent use of this platform to achieve our educational and promotional objectives. A notable example is the publication of a report on completion of an investigation into a complaint or an investigation initiated by us. This serves multiple purposes. First, it encourages data users to promptly and genuinely engage with the resolution of privacy issues to avoid adverse publicity. Secondly, it warns individuals and other data users of the practices of the data user. Thirdly, it promotes public discussion thereby enhancing privacy awareness and compliant behavior. Since 1997 we have published 23 investigation reports, of which 10 were published during my tenure in the past 18 months.

More importantly, I have since June 2011 adopted the policy of naming in a published investigation report the corporate data user which has contravened the legal requirements. This practice serves to invoke the sanction and discipline of public scrutiny and in turn will encourage even more effectively compliant behavior by both the data user being the subject of investigation and other data users facing similar investigation issues.

Partnership with other Regulators

The media is no doubt a very good partner in promotion and educational work.

On the enforcement side, recognizing the limits of my enforcement power, I have resorted to partnering with other regulators, leveraging their legislative mandates, institutional tools and enforcement powers. Where appropriate, I will send an advance copy of my published investigation report to the relevant regulatory body to see what additional regulatory or advisory functions they could exercise in respect of the data user at fault or the industry concerned.

For example, the Octopus incident revealed that the unauthorized transfer of customers' personal data to third parties for direct marketing purposes or 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, namely, the Hong Kong Monetary Authority, the Telecommunications Authority and the Commissioner of Insurance, 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 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.

More recently, a property agency and an estate agent were together convicted of contravention of section 34(1)(ii) of the Ordinance, which requires a data user to stop using an individual's personal data for direct marketing purposes upon receipt of an opt-out request. The case was referred to the Estate Agents Authority which has been very active in promoting among the estate agency practitioners the importance of protecting clients' personal data. It issued a new practice circular in this regard, which took effect on 1 October 2011. A practitioner who breaches

the guidelines in the practice circular may be subject to disciplinary action.

Partnership with other Enforcement Agencies

May I recap that when we come across a prima facie case of an offence under the Ordinance, we have to refer to the Police and the DoJ for criminal investigation and prosecution. Our record of successful prosecution has not been impressive. Since the Ordinance came into effect in 1996, there have been only 14 convictions, that is, less than one conviction per year. This is understandable as privacy and data protection have apparently not been accorded top priority on the agenda of these two government departments.

To address this situation, I have had a serious discussion early last year with the Police and the Director of Public Prosecution. The meeting turned out to be fruitful as it culminated in the streamlining of the referral procedures and the joint formulation of policies and guidelines for the handling of referred cases. In the past 12 months, we recorded a total of 4 convictions.

Partnership with Overseas Counterparts

Data protection is a global mission. As at today, a total of 89 jurisdictions have data protection laws. So, Hong Kong is not fighting a lonely battle. International cooperation in data protection is important, particularly in view of the prevalence of cross-border data transfer and the borderless operations of global corporations as well as Internet and mobile services providers.

My office is a member of the International Conference of Data Protection and Privacy Commissioners. We are committed to improving cross-border co-operation in each member's enforcement of its national laws in data protection.

At a regional level, Hong Kong is part of the Asia-Pacific Privacy Forum, an informal network of privacy enforcement authorities which meet twice

a year to foster co-operation, share information, discuss operational strategies, promote best practices, and support joint awareness raising campaigns.

In terms of regional enforcement cooperation, I should point out that Hong Kong is a member of the APEC Cross-border Privacy Enforcement Arrangement (CPEA) which commenced in July 2010 and include the data protection authorities from Australia, Canada, Japan, New Zealand and U.S. This co-ordination framework will help in my investigation of violation of personal data privacy that involves cross-border data transfer. I can contact other participating authorities for assistance through referral of matters and through parallel or joint investigations or enforcement actions.

Partnership with Civil Society

Last but not the least, I fully appreciate that the civil society is a strategic partner that we have to collaborate with in the pursuit of our mission.

I know today's event is sponsored by Privacy International, the very first civil organization to campaign on privacy issues at the international level. I know the participants of today's symposium come from a diverse background, including academics, legal professionals and civil rights advocates. I really appreciate your attendance. Your interest in privacy and data protection is a great source of inspiration for my work as the Privacy Commissioner.

In return, may I invite you to meet up with my counterparts from the Asia Pacific region, who will come to Hong Kong in mid-June this year for the Asia Pacific Privacy Authorities Forum. I shall arrange a special discussion session between these overseas friends and the privacy advocates in Hong Kong. Professor John Bacon-Shone has kindly consented to lead the discussion. So you can either contact him or me for enrolment. I am sure we will have a fruitful exchange.

With this offer, I will end my presentation. May I wish you an enjoyable and rewarding symposium today. Thank you very much.