Seminar on Consultation on

Review of the Personal Data (Privacy) Ordinance

Why the review is being conducted and what this means to you

On 28 August 2009, the Government released the Consultation Document on Review of the Personal Data (Privacy) Ordinance. The theme of today's seminar is "Why the review is being conducted and what this means to you?" It is my plan to start this keynote address by giving you some background information of the Ordinance review exercise.

Background

2. The Ordinance was enacted in 1995 and its core provisions came into operation on 20 December 1996. Although Hong Kong is pioneer in Asia in implementing a mature piece of data protection legislation, the rapid technological and e-commerce developments that are taking place in this electronic era and the exponential rate with which it continues to progress give rise to global privacy concern.

3. After I took up the office of Privacy Commissioner in August 2005, I noticed that piecemeal legislative amendments

canvassing mainly technical matters had been put forward by my predecessors to the Government for consideration at various times since 1998. But none of the amendments proposed by them had been tabled before the Legislative Council for vetting. At international level, overseas governments and privacy regulators were at various stages of reviewing and reforming their privacy laws in order to safeguard the personal data privacy interests of the individuals. Australia, Canada, New Zealand and United Kingdom have been engaged in privacy law reviews. Instead of simply pushing the Government to obtain legislative time slot for piece-meal amendments which might or might not happen during my term of office, I decided that a holistic review of the Ordinance is the preferred course of action having regard to the ever increasing privacy risks posed by technological transformation. This may well be a job for the Law Reform Commission but I did not want to wait. If the Ordinance does not keep pace with international developments and if the adverse privacy impact caused by modern technologies is left unaddressed, Hong Kong will lose its competitive edge to other countries in the region. A legislative amendment exercise has to be undertaken so that our privacy law can provide adequate protection to personal data privacy in this electronic information age.

4. With this objective in mind, I set up an internal Ordinance Review Working Group was formed in June 2006. Our mission was to come up with a comprehensive set of legislative amendment proposals for Government's consideration. The Working Group took into account the following factors in the course of the review:-

(a) the sufficiency of protection and the proportionality of penal sanction under the Ordinance;

(b) the development of international privacy laws and standards since the operation of the Ordinance;

(c) the regulatory experience of the Office of the Privacy Commissioner gained in the course of discharging its functions and powers;

(d) the difficulties encountered in the application of certain provisions of the Ordinance;

(e) the technological development in an electronic information age facilitating the collection, holding and processing of personal data in massive quantum at a low cost;

(f) the development of biometric technology for the identification of an individual poses challenges to the maintenance of individuals' privacy; and

(g) the vulnerability of individuals in becoming less able to control and determine the collection, use and security of his personal data stored and transmitted through electronic means.

Missions

5. The Working Group had five missions to achieve in undertaking the review exercise. They were:-

- To address issues of public concern.
- To safeguard personal data privacy rights while protecting public interest.
- To enhance the efficacy of regulation under the Ordinance.
- To harness matters that will have significant privacy impact.
- To deal with technical and necessary amendments.

6. After a year and a half's work, the Working Group completed its review and presented to the Government in

December 2007 more than 50 amendment proposals and issues of privacy concern. Since then, more than a year and a half have been spent by us explaining to the Administration and discussing the proposals.

7. The Administration has taken on board most of the proposals made by my Office but rejected a few. I have succeeded in persuading the Administration to include in the Consultation Document those proposals that it does not support so that the general public will have a chance to comment on those proposals. These proposals can be found in Annex 2 of the Consultation Document and they include the following:-

- ~ Granting Criminal Investigation and Prosecution Power to the PCPD
- ~ Imposing Monetary Penalty on Serious Contravention of Data Protection Principles
- ~ To Award Compensation to Aggrieved Data Subjects
- ~ Creation of an offence of repeated Contravention of a Data Protection Principle on Same Facts
- ~ Increasing the penalty of Repeated Non-compliance with Enforcement Notice
- ~ Creation of a new exemption of Public Interest Determination

~ Revamping Regulatory Regime of Direct Marketing

8. Although the Government does not support the above proposals, it is your privilege to voice out your concerns, to make your own submissions and to help shape the new data protection law that protects everyone of us in the future.

9. My Office has prepared a paper entitled *"PCPD's Information Paper on Review of the Personal Data (Privacy) Ordinance"* which provides additional information for the public to consider before making their submissions to the consultation. The paper contains the original proposals made by the PCPD to the Government as well as relevant issues of privacy concern. It is available at the PCPD's website at www.pcpd.org.hk.

Highlights of the Proposals

10. With your permission, I now proceed to highlight in details some of the proposals made by my Office.

11. In recent times, a series of incidents involving leakage or loss of sensitive personal data has caused grave privacy concern, for instance, the IPCC leakage of complainants' personal data, on-line dissemination of the nude photos and the

loss of patients' data by the Hospital Authority. While there are at present provisions under the Ordinance regulating data users in safeguarding data security, I find that it is timely to strengthen its provisions to enhance the protection of personal data privacy.

12. In order to curb irresponsible dissemination of leaked personal data, I proposed to make it an offence for any person who knowingly or recklessly, without the consent of the data user, obtains or discloses personal data held or leaked by the data user. I also proposed to make it illegal for anyone to sell the personal data so obtained for profits.

13. In relation to the transfer of personal data to an outsourced agent or contractor for handling, I proposed to impose an obligation on data users to use contractual or other means to provide a comparable level of security protection measures when personal data are entrusted to third parties engaged for handling personal data. I further proposed that data processors should be obliged to observe the requirements of Data Protection Principles 2(2) (duration of data retention), DPP 3 (use of personal data) and DPP 4 (security of personal data), thereby imposing appropriate regulatory control over them.

14. To mitigate or reduce the damage that may be caused to data subjects whose personal data are leaked or lost, I suggested that the Administration should consider making privacy breach notification mandatory so as to require the data users to promptly notify individuals who are affected by the loss or theft of personal data in certain breaches where there was a high risk of significant harm. My Office should also be notified of the relevant events when such events happened.

15. The Ordinance as it presently stands does not differentiate personal data that are sensitive from those that are not. However, certain kinds of personal data are by their inherent nature commonly taken as more sensitive. I proposed to the Government to bring the protection level of special categories of personal data at par with the standard stipulated in the EU Directive 95/46/EC on Guidelines on *the Protection of Privacy and Transborder Flows of Personal Data*. I suggested that the new definition of "sensitive personal data" could include the racial or ethic origin of the data subject, his political affiliation, his religious beliefs and affiliations, membership of any trade union, his physical or mental health or condition, his biometric data and his sexual life. Special care are warranted in the proper handling of sensitive personal data in view of the gravity of harm that may cause the data subjects as a result of mishandling of those data. In anticipation of the eventual

implementation of electronic patient records where massive sensitive health records are kept in databases for use and access, I consider that more stringent controls and prudent practice should be required. Hence, I proposed that special treatment be applied to the handling of "sensitive personal data" and that prior to their collection from data subjects, the latters' consent should be sought.

16. I also made proposals which aim at making the legislative mechanism more robust. At present, a person who contravenes any data protection principle faces no sanction unless he does so in non-compliance of an enforcement notice issued by the Commissioner. An aggrieved individual may indeed make a civil claim against the data user under section 66 of the Ordinance for compensation, I am not aware of any award of damages having been made by the court since the commencement of the Ordinance. Taking the IPCC case as an example, the affected individuals have to take civil actions by themselves in order to obtain compensations for leakage of their personal data. Only very few individuals have initiated legal proceedings, none of which seems to have gone to trial. There is ample ammunition for those who criticize that the Ordinance is deficient and ineffective in affording remedies to aggrieved individuals or deterrence. For these reasons, I proposed to confer power on the Commissioner to require data users to pay

monetary penalties for serious contraventions of data protection principles. A similar power is vested in the Commissioner in the U.K. under Section 55A of Data Protection Act. I further proposed to confer power on the Commissioner to award compensation to the aggrieved data subjects. A similar provision exists in the Australian Privacy Act. Even if all the above proposals are not considered appropriate here in Hong Kong, I also suggested that the Commissioner may include as one of his functions to provide legal assistance to persons who intend to institute legal proceedings under the Ordinance.

17. The commercial value of direct marketing activities is well known. However, the flourishing of such activities sometimes result in unwelcome calls and cause nuisance to the recipients. The regulatory regime under section 34 of the Ordinance is to require the direct marketers to give an "opt-out" choice to the data subject when first using his personal data for such purpose. Repeated direct marketing activities to a person who has "opted out" from such activities constitutes a breach of the provision of the Ordinance which amounts to an offence. In reviewing the effectiveness of the Ordinance to tackle the problem, I would like to know the views of the public as to:-

i. whether an "opt-in" instead of "opt-out" regime is more appropriate;

ii. whether a territorial-wide central Do-not-call register be established and

iii. whether a data user shall be required to disclose the source of the recipient's personal data upon the latter's request. The penalty level should also be reviewed.

Global approach

18. The host of this conference has asked me to talk about how privacy law will develop. For future development, I would refer anyone who is really interested to the recent report released by the UK Information Commissioner's Office on the Review of the European Data Protection Directive in May 2009. The report concludes that, in an increasingly global, networked environment, the Directive will not suffice in the long term. The report acknowledges that the Directive has helped to harmonise data protection rules across the European Union and has provided an international reference model for good practice. However, the report also says that the Directive is often seen as burdensome and too prescriptive, and may not sufficiently address the risks to individuals' personal information.

19. The threat to data privacy in future arises from the seamless flow of personal data across borders stemming from the proliferation of e-commerce and outsourcing activities.

These cross-border data flows demonstrate the degree to which territorially-based privacy regulation is rapidly becoming ineffective. In this atmosphere, cooperation between regulators in different geographic jurisdictions, as well as mechanisms for businesses to develop uniform standards, such as the Asia–Pacific Economic Cooperation (APEC) Privacy Framework are becoming increasingly relevant.

20. The APEC Privacy Framework was developed by the Data Privacy Subgroup under the APEC Electronic Commerce Steering Group. The aim is to establish a commonly accepted privacy protocol within the APEC region in the context of e-commerce. Since 2003, my Office has participated in the work of the Data Privacy Subgroup, providing comments and opinions from the perspective of a privacy regulator. In 2007, the APEC Ministers endorsed the Data Privacy Pathfinder in working together by pursuing multiple projects to create implementation frameworks to achieve the goal of creating a foundation of trust that promotes accountable data flows across the APEC region, specifically by using Cross-Border Privacy Rules. This year will be a milestone. The Data Privacy Subgroup aims to have the APEC Cross-Border Cooperation Arrangement endorsed by the APEC Ministers in November 2009. Member economies may then participate in the arrangement which facilitate cross-border cooperation on

enforcement of privacy laws complaints on infringement of personal data privacy.

21. In the future, what will be the best method of protecting individuals' data in international transfers? There is no single solution. One of the optimal ways to protect the cross border safe transfer of personal data is the existence of a mature piece of privacy legislation both in the sending countries or regions and the recipient ends. Personal data privacy is protected where the handling of the data is regulated by requiring compliance with statutory data protection principles, overseen by a regulatory authority or enforced through sanction. In Hong Kong, for instance, its privacy legislation has stipulated the circumstances for transfer of personal data to places outside Hong Kong, though the relevant provision (section 33) is not yet operative. In the absence of local privacy legislation, the subscription to an internationally accepted privacy standard and practice by countries and regions is conducive to the cross border flow of personal data in a data protective framework. Continuous efforts should be made by the countries and regions in developing a set of global privacy principles and practice to be commonly adopted by the governments and business sectors for promoting e-Government and e-Commerce, for example, data breach notification. Cross-border cooperation in privacy enforcement is also a step forward to enhancing the protection

of personal data that are transferred in the borderless world of the Internet.

Conclusion

22. Modern approaches to regulation of personal data protection mean that laws must:-

i. concentrate on the real risks that people face in the modern world,
ii. avoid unnecessary burdens, and
iii. work well in practice.

23. Technological advances, proliferation of e-commerce and the need for transfer of personal information across borders all signal the need for the law to evolve. While striving to be technologically neutral, our law has to be reviewed to ensure that it is capable of coping with these challenges. To operate successfully, a privacy law has to balance the duties of data controllers and the rights of the individuals. Since personal data privacy law is an evolving concept, continuous efforts have to be made to react positively to the changing needs of any particular society and to harness the privacy challenges posed by technological advancements.

24. May I end my address with an appeal to anyone, data user or data subject, and they can often be the same person, who is interested in the proper protection of personal data to respond to the Consultation which ends on 30 November.

END