Review of the Hong Kong Personal Data (Privacy) Ordinance :
From the perspective of Hong Kong Privacy Commissioner

1. The Hong Kong SAR Government recently issued a Consultation Document on Review of the Personal Data (Privacy) Ordinance ("the Consultation Document") containing 43 proposals. Views and comments are invited on the proposals in Annex 1 of the Document. Annex 2 of the Document contains the proposals which the Government is disinclined to pursue. The remaining proposals in Annex 3 are proposals which address technical and operation problems encountered in the implementation of the Personal Data (Privacy) Ordinance ("the Ordinance"). The consultation ends on 30 November 2009 giving the public some three months to respond.

Background

2. The core provisions of the Ordinance came into operation in December 1996. Although Hong Kong remains the only jurisdiction in Asia with a mature piece of data protection legislation and a privacy commissioner, the rapid technological and e-commerce developments and the exponential rate with which it continues to progress have given rise to genuine privacy concerns.

3. Piecemeal suggestions for legislative amendments canvassing mainly technical matters had in the past been put forward to the Government. They were exercises in futility since no legislative time slots could be found for what appeared to be less than significant changes.

4. Soon after I took office in August 2005, I realized that if our privacy law was not seen to keep pace with international developments and if the adverse privacy impact caused by modern technologies was not sufficiently addressed, Hong Kong would suffer. A holistic approach, and not a partial legislative amendment, has to be adopted. My aim is to bring our privacy law up to date so that the personal data of the 7 million individuals in this metropolis can enjoy adequate protection.

5. With this objective in mind, I formed an internal Ordinance Review Working Group in June 2006. We toiled away for a year and a half. On the eve of Christmas 2007 I was able to present the Government with a package of some 50 proposals. The proposals reflected the various factors which the Working Group had taken into account, namely, the development of international privacy laws and standards since the operation of the Ordinance; the regulatory experience my office has gained in the past, particularly the difficulties encountered in the application of certain provisions of the Ordinance; and the vulnerability of individuals who have become less able to control and determine the collection, use and security of their personal data stored and transmitted through electronic means.

6. I recognize that any major change to the law must address current issues of public concern, balance privacy right against public interest and harness matters that will have a significant privacy impact. Above all, the efficacy of regulation is as important as the words on the statute book.

7. The Government took some convincing but eventually came out in support of most of the proposals, modified a few and for its own reasons rejected the rest.

8. The Consultation Document contains some 80 pages and the consulting public can obviously do with a lot more reference materials in their preparation of a meaningful response. I therefore uploaded on my official website a condensed collection of materials my Working Group had assembled and prepared. The name which I have given to this collection is *"PCPD's Information Paper on Review of the Personal Data (Privacy) Ordinance"*. The materials include the proposals made to the Government in December 2007.

Main proposals

9. The scope of the review exercise is extensive. I shall here restrict myself to some of the main proposals which, if implemented, will have a significant and fundamental impact on personal data protection in Hong Kong.

10. In recent years, various incidents involving leakages or losses of sensitive personal data have caused grave privacy concern. Still fresh in the

public mind include the Independent Police Complaints Council's leakage of the personal data of hundreds of citizens who had complained against the police and the losses of patients' data by public hospital under the management of the Hospital Authority. All these have given rise to the call for increased efforts to enhance personal data protection.

Sensitive Personal Data

11. The Ordinance as it stands does not differentiate personal data that are sensitive from others. The EU Directive 95/46/EC on Guidelines on *the Protection of Privacy and Transborder Flows of Personal Data* and other overseas privacy legislations provide specific protection for special categories of personal data including racial or ethnic 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. In response to my suggestion to bring the level of protection at par with overseas standard, the Government indicates that as a start only biometric data should be classified as sensitive personal data. In my recent response to the Consultation Document I urged the Government to review its decision and in particular I consider that medical data should be included as sensitive data. It remains to be seen what the public view is.

12. In my proposal I suggest that the collection, holding, processing and use ("handling") of sensitive personal data ought to be prohibited except in certain prescribed circumstances: (a) with the prescribed consent of the data subject, (b) it is necessary for the data user to handle the data to exercise his right as conferred by law or perform his obligation as imposed by law, (c) it is necessary for protecting the vital interests of the data subjects or others where prescribed consent cannot be obtained, (d) handling of the data is in the course of the data user's lawful function and activities with appropriate safeguard against transfer or disclosure of personal data without the prescribed consent of the data subjects, (e) the data has been manifestly made public by the data subjects, (f) handling the data is necessary for medical purposes and is undertaken by a health professional or person who in the circumstances owes a duty of confidentiality, and (g) handling of the data is necessary in connection with any legal proceedings.

13. Many stakeholders have expressed concerns on the possible adverse

effect and confusion the proposal may bring. They fear a reduction in business opportunities. However, the proposal does envisage a transitional period. Perhaps in the long run, the public will support the view that personal data privacy right should be properly balanced with but not be sacrificed too readily in the interest of economical gains.

Data Processor

14. At present, the Ordinance does not directly regulate the activities of data processors. I propose that they be brought accountable under the Ordinance. In addition, I suggest that data users should be obliged to use contractual or other means to ensure that the data processors to whom they entrust the personal data will provide a level of security comparable to their own obligations. Data processors should be required to observe the requirements of Data Protection Principles ("DPP") 2(2) (duration of data retention), DPP 3 (use of personal data) and DPP 4 (security of personal data).

Breach Notification

15. In the wake of a large number of data leakage incidents and the damage caused to the data subjects, I propose that a notification mechanism be put in place. In the Consultation Document, the Government considered introducing voluntary notification mechanism that requires data users to promptly notify individuals who may be affected by a data breach so that they can take early steps to protect themselves and minimize their exposure to potential damage or risk of identity theft or fraud. The proposal requires data users to adopt a risk-based approach to notify incidents that carry a real risk of harm. My office should also be informed of such breaches so that compliance checks can be carried out and where appropriate, timely guidance can be given to the data users concerning the security of their systems.

16. I am asking the Government to consider making data privacy breach notification mandatory so as to afford greater protection to personal data privacy right. At this stage, it seems to me that the Government is inclined towards a voluntary notification mechanism, at least for a start.

Unauthorised Obtaining, Disclosure and Sale of Personal Data

17. To curb irresponsible dissemination and misuse of leaked personal data, I propose making 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 further propose to make it unlawful for anyone to sell the personal data so obtained for profits. Both of these proposals are modeled on the U.K. Data Protection Act.

18. Applicable defences for the proposed offences should include (a) necessary for preventing or detecting crime, (b) required or authorized by an enactment, rule of law or court order, (c) acted in reasonable belief that he had in law the right to obtain, disclose or procure the disclosure, (d) acted in reasonable belief that he would have had the consent of the data user if the data user had known of the act, (e) justified as being in the public interest, (f) acted for specific purpose, with a view to publication by any person of any journalistic, literary or artistic material and in the reasonable belief that such act was justified as being in the public interest.

19. The Government stresses in the Consultation Document that the offences should be confined to such culpable acts for "profits" or with "malicious purposes". An offender will be fined that accords with the gravity of the offence. I disagree with the narrow scope set by the Government since it will hardly cover the loophole of the existing legal framework highlighted in the recent acquittal of a tax officer who collected the personal data of 13,400 individual tax-payers. The employee was charged with one count of misconduct in public office, contrary to Common Law. However, the court found that the intended purpose of use was not proved and that the collection had not brought the employee any financial gain.

Award of Compensation and Monetary penalty

20. 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 Privacy Commissioner. An aggrieved individual may make a civil claim against the data user for compensation by reason of a contravention of a requirement under the Ordinance. Since the commencement of the Ordinance, there has not been a single court award of damages. This in my view is highly unsatisfactory. To enhance the effectiveness of affording

remedies to aggrieved individuals and achieve greater deterrence on privacy intrusive act or practice, I propose that the Privacy Commissioner be given the power to award compensation to an aggrieved data subject, subject of course to an appeal procedure being in place. Not much to my surprise, this proposal is not being supported by the Government.

21. I also propose that the Privacy Commissioner be vested with the power to require data users to pay monetary penalties for serious contraventions of the Data Protection Principles.

Legal Assistance

22. In anticipation of the above two proposals not being accepted, I have also asked the Government to support legislative amendments to enable me to provide legal assistance to aggrieved data subjects who intend to institute legal proceedings against data users. This last proposal appears to be favoured by the Government.

Direct Marketing

23. The flourishing of direct marketing activities often results in unwelcome calls and nuisance to the recipients. The current regulatory regime 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" constitute a breach of the Ordinance which amounts to an offence. There are criticisms that the existing penalty level for such an offence is too low and should be raised.

24. As a related proposal, I have suggested to the Government consideration whether an "opt-in" regime be preferred to an "opt-out" regime and whether a territory-wide central do-not-call register be established; and whether a data user should be obliged to disclose the source of its collection of the personal data of whom it calls.

Conclusion

25. I have posted onto my official website my formal response to the

Government's Consultation Document. I hope the public participation in the consultation exercise will reflect fully the views of all the stakeholders. In time my colleagues and I look forward to a rejuvenated privacy law that can satisfactorily meet the challenges that the digital age has brought and will bring.

Roderick B. Woo
Privacy Commissioner for Personal Data, Hong Kong