Skeleton Submission by Roderick B WOOat a special meeting of the Legislative Council's Panel on Constitutional Affairs to be held on 20 November 2010 in relation to the Government's Consultation Report on its Public Consultation on Review of the Personal Data (Privacy) Ordinance

Background

1.1 In December 2007 I, in my capacity as the Privacy Commissioner for Personal Data ("PCPD"), presented a report to the Secretary for Constitutional and Mainland Affairs urging that the Ordinance be holistically reviewed and amended. I put forward more than 50 proposals with supporting research materials and justifications for the Government's consideration. In August 2009 the Government responded to my report and published a Consultation Document to seek views from the public. The PCPD made a written submission in November 2009.

1.2 The Government has now presented its Consultation Report before the Panel on Constitutional Affairs. As the instigator of PCPD's original proposals and as a concerned member of the public with special expertise and experience on personal data privacy protection, I wish to contribute to the discussion of the Consultation Report and take the opportunity to persuade the Government to reconsider its current stance on some of the proposals.

1.3 For the purpose of this Skeleton Submission, I shall divide the proposals into three parts, namely, (A), (B) and (C).

(A) Newly introduced proposals to regulate direct marketing

2.1 In the wake of the Octopus Card case, the Government has introduced **Proposal (1)** in relation to the collection and use of personal data in direct marketing. This proposal did not appear in the Consultation Document and the public has not been consulted on it.

2.2 Direct marketing is one of the recognized modes of promoting the sale of merchandise and services in Hong Kong. In PCPD's submissions in December 2007, I made the following comments :

"Direct marketing has significant commercial value in promoting the products and prospering the businesses of commercial entities. However, the proliferation of uncontrolled direct marketing activities cause nuisance and annoyance to individuals and encourage the sale of personal data in bulk which infringes the personal data privacy of the data subject, particularly his right 'to be left alone'".

2.3 I suggested that consideration be given as to whether the data user is required to provide an "opt-in" choice to the data subject before his personal data are used for direct marketing for the first time. I then went on to make reference to the feasibility of setting up a "do-not-call" register against direct marketing activities in the same way the Unsolicited Electronic Messages Ordinance has done. I stated that my disposition was "open-minded" and proposed that the public be consulted on this issue.

2.4 The Government's Consultation Report suggests that there is a significant view that the existing "opt-out" arrangement, as opposed to an "opt-in" arrangement, is preferred. On balance, I am inclined to give weight to such a significant view and support the new Proposal (1) that additional specific requirements be introduced to effect stricter regulation on data users in their use (including transfer) of the personal data collected for direct marketing purposes.

2.5 Regarding **Proposal (2)** in relation to unauthorized sale of personal data by data users, I agree to the Government's proposal to impose additional requirements and the creation of certain offences. The reason is that such sale, if left unregulated, will expose the personal data transferred in the course of the sale to further risks of improper uses. In drafting the offence provisions, careful consideration should be given to the following:

(i) a clear definition of "unauthorized sale";

(ii) the processing of such data by sub-contractor of the direct marketers, which might involve monetary or in kind gain; and

(iii) what defence should be made available to the data user?

2.6 The opt-out right to be given to the data subjects upon collection of the personal data should not overlook the facts:

(i) that some direct marketing activities are directly related purposes of collection of the personal data that may fall within the reasonable expectation of the data subjects;

(ii) that data subjects should be given the opt-out right to choose any one or more of the direct marketing purposes that he disagrees; and

(iii) that such opt-out right is to be separately provided so that the individual can clearly indicate his preferences.

2.7 Consideration should be given to the establishment of a central do-not-call register to cover person-to-person calls by extending the scope of the Do-Not-Call Register currently implemented under the Unsolicited Electronic Messages Ordinance to facilitate individuals in expressing their preference as well as a channel for checking by the direct marketing companies before making approaches to individuals.

(B) Proposals which the Government put forward for consultation but does not now intend to pursue

3.1 Of the proposals which the Government put forward for consultation in 2009, seven will not now be taken forward. I regret to note that such proposals are abandoned and urge the Government to reconsider them, in particular, the proposals on **sensitive personal data** and the **giving of additional powers to the PCPD**.

Proposal (38) : sensitive personal data

3.2 The Government in the Consultation Document has this to say :

> *"3.02 More stringent regulation of sensitive personal data is in line with international practices and standards. The European Union Directive 95/46/EC on the "Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data ("EU Directive"), which regulates the processing of personal data within the European Union, contains provisions to subject the processing of sensitive personal data to extra restrictions. The legislation of some overseas jurisdictions, such as the Data Protection Act 1998 of the United Kingdom ("UK Data Protection Act") and the Privacy Act 1988 of Australia ("Australian Privacy Act"), contains specific provisions regulating the handling of sensitive personal data."*
>
> *"3.05 From the perspective of data protection, a higher degree of protection should be afforded to sensitive personal data given the gravity of harm that may be inflicted upon the data subject in the event of data leakage or*

accidental disclosure to third parties. Limiting the handling of sensitive personal data to specified circumstances would narrow down the scope of collection and use of such data, thus providing better safeguard against indiscriminate use and inappropriate handling."

3.3 Plainly, the Government agrees that certain data should be regarded as sensitive personal data. It proposed that for a start, biometric data be singled out as a type of sensitive personal data to be under stricter legislative control. Even in the Consultation Report now before the Panel, it is said that:

"4.2.8 Most of the views expressed in various consultation activities and in submissions received agree with the general direction of providing a higher degree of protection to sensitive personal data. …"

"4.2.14 Most of the views suggest that there should be a clear definition of sensitive personal data and some suggested that a set of sensitive personal data be specified. …"

"4.2.15 Some participants in the public consultation activities proposed that a set of principles should first be developed to define sensitive personal data …"

3.4 It seems that both the Government and the general public agree that some data, such as health records, credit data, criminal records, etc. should be more carefully handled and processed as the damage and harm caused to the data subjects on improper handling can be irreparable and far reaching. By way of illustration, the Government is particularly conscious of the need of affording special protection to patients' medical records in its present endeavours to introduce the Electronic Health Records Sharing System.

3.5 I was disappointed that instead of consulting the public what should be considered sensitive personal data, the Government's original proposal singled out only biometric data as "sensitive data". Not unsurprisingly, the Government met with strong opposition from the information technology sector on this proposal. The Government has again disappointed me by its decision to simply give up all intentions of making any legislative change to the Ordinance to bring to the attention of data users the importance of treating sensitive personal data with greater care. To me, this is incomprehensible in the light of the Government's original resolve and the positive public response (as shown in the excerpts above quoted) that "sensitive personal data" should be under stricter control. My suggestion is that the least Government should now do is to take the first step in the right direction by proposing that a new regime under which sensitive personal data would be receiving

special attention. A list of "sensitive data" can be compiled *via* a gradual process which should include a wide public consultation over a period of time. This move should have the effect of making the legislative recognition that special treatment shall be accorded to some personal data and paves the way to specific personal data to be admitted into that category in the future.

3.6 In the absence of stricter legislative protection being given to sensitive personal data, Hong Kong is placed at a disadvantage when compared with the EU and international standards. This will have the adverse effect of hindering the free flow of personal data to Hong Kong.

3.7 The Government is suggesting that the PCPD should issue codes of practice or guidelines on best practices. Neither of these has the force of law and that breaches of the same are not contravention of the Ordinance *per se*. I therefore urge the Government to reconsider the proposal.

Granting criminal investigation and prosecution power to the PCPD

3.8 I continue to support this proposal as outlined in the PCPD's 2007 report and its submission to the Consultation Document in November last year. The reasons are clearly stated in both documents. It has to be borne in mind that performing its statutory functions, the PCPD has consistently done work which can be regarded as partial criminal investigation. As to the functions of a prosecutor, it is simply a job of presenting to the judicial body all the relevant facts of the case. Such a capacity should not be confused with judging whether a criminal offence has been committed and by whom. The power to judge always stays with the court alone. The argument that PCPD should not act both the accuser and the jury simply cannot be sustained.

Proposal No. 6 : empowering the PCPD to award compensation to aggrieved data subjects

3.9 Civil remedy under section 66 of the Ordinance is costly to pursue as witnessed by the fact that no court has been known to have tried or considered an application for compensation to an aggrieved data subject. Members of the public, including members of the Legislative Council, are scornful of the powerlessness of the Privacy Commissioner, even in blatant cases of contravention of the Ordinance, apart from serving an Enforcement Notice on the culprits. In particular, there is a

sense that justice is not done especially in cases where data users have made huge profits or gains by manipulating the personal data they have collected.

3.10 The power to award compensation by the Privacy Commissioner will address such concern. Armed with such power, the PCPD can act as a mediator bringing results which satisfy both the data user and the data subject concerned. The PCPD's original proposal envisaged that the exercise of such power would be stringently regulated and subject to appeal. I therefore urge the Government to reconsider this proposal.

Proposal (6): Personal Data Security Breach Notification

3.11 While this Proposal is included as one of the proposals taken forward by the Government in the Consultation Report, it does not recommend a change of the law which currently does not call for a mandatory rendering of a breach notification. That being the case, it is a mistake for this Proposal to come under the heading of "(A) Proposals to be Taken Forward" in the Government's Consultation Report.

3.12 I maintain the stance I took in the PCPD's submissions in November 2009 that breach notification ought to be made mandatory. I suggest that initially only data users in the public sector be legally required to give breach notifications. This should not cause any problem as the Government has required these users to give breach notifications on a voluntary basis for well over a year now. I was and am conscious of the likely concerns on the part of data users in the private sector on the imposition of this new requirement and I made the following comments in the PCPD's Submissions last November :-

> *"3.27 There are concerns that it may cause the private sector undue burden to comply with the proposed requirements. It should be noted that under the proposed mechanism, a data user is not required to notify every security breach. It is only in cases where the security breach may result in high risk of significant harm to individuals or organizations that notification is required. The PCPD will issue guidelines on the circumstances that would trigger the notification as well as the particulars to be contained in the notice."*

3.13 I also suggested in the Submissions that the requirement be applied to selected classes of data users in the private sector on a step by step process to be determined by the PCPD. The selection process should be guided by a number of factors including the amount of personal data held by the specified class of data

users, the degree of sensitivity of the data, the risk of harm to the data subjects as a result of the breach.

(C) Proposals not pursued by the Government at the outset

4.1 Of the PCPD's original proposals which the Government does not intend to pursue, I wish to highlight the following and strongly urge the Government to reconsider its position.

The power to conduct hearing in public

4.2 Section 43(2) of the Ordinance provides that:

> *"Any hearing for the purposes of an investigation shall be carried out in public unless –*
> *(a) The Commissioner is of the opinion that, in all the circumstances of the case, the investigation should be carried out in private; or*
> *(b) If the investigation was initiated by a complaint, the complainant requests in writing that the investigation be carried out in private."*

4.3 It is obvious that the spirit of the legislation is that the hearing, as a matter of principle, be in public. The exception in section 43(2)(b) is to afford confidentiality or secrecy to the complainant. The best way out must be for the Privacy Commissioner to have that part of the hearing concerning the complainant to be in camera and otherwise be anonymized. For cases of great public concern, the holding of hearings in public by the Privacy Commissioner will serve the purpose of fairness and transparency and members of the public can have real time access to the progress of the investigation. The public hearing in relation to the Octopus Card casein last July is a case in point. I therefore ask the Government to reconsider this proposal.

Time limit for responding to PCPD's investigation or inspection report

4.4 Section 46(4) of the Ordinance requires the Privacy Commissioner, before publishing an investigation / inspection report, to allow a data user a period of 28 days to object to the disclosure of any personal data in the inspection / investigation report that are exempt from the provisions of DPP6.

4.5 In practice, the inspection / investigation reports have not in the past contained any personal data as the names of the relevant data user and other individuals involved are not normally be disclosed. The 28 days requirement as presently worded in the Ordinance is an unnecessary delay and burden to the proceedings undertaken by the PCPD. The recent investigation in the Octopus Card case and the inspection of the Hospital Authority's patients data system carried out by PCPD in 2008 are both cases of strong public interest and the publication of PCPD's reports containing no personal data were delayed because of this 28 days requirement.

4.6 I suggest therefore that the Ordinance be amended so that this 28 days requirement does not have to apply to reports which do not contain personal data.

End Notes

5.1 I am appreciative of the Government's efforts in responding positively to most of PCPD's proposals and for the work that it has undertaken in reviewing the Ordinance with the PCPD and conducting the public consultation.

5.2 This paper is prepared only for the purpose of this occasion. After listening to and considering the views of all parties concerned including any revision on the part of the Government of its current stance, it is my intention to submit a fuller paper in response to the invitation contained in the Consultation Report before 31 December 2010.

5.3 I look forward to a timely improvement on and updating of the Ordinance. I hope the Government will soon announce a time-table leading to the tabling of a Bill before the Legislative Council to effect a holistic amendment of the Ordinance.

Roderick B WOO

Dated 19 November 2010