LC Paper No

LEGISLATIVE COUNCIL

Bills Committee

Personal Data (Privacy) (Amendment) Bill 2011

Purpose

This paper briefs Members on the views of the Privacy Commissioner for Personal Data ("**PCPD**") regarding the Personal Data (Privacy) Amendment Bill ("**Amendment Bill**") submitted by the Constitutional and Mainland Affairs Bureau ("**CMAB**") to the Legislative Council on 13 July 2011.

Background

2. After two rounds of public consultation and discussions on the various proposals for the review of the Personal Data (Privacy) Ordinance ("**Ordinance**"), CMAB published the "Report on Further Public Discussions on Review of the Personal Data (Privacy) Ordinance" ("**Further Discussion Report**") in April 2011. The Further Discussion Report reaffirmed that CMAB would pursue the majority of the proposals previously submitted by PCPD. New requirements and offences will be introduced to regulate the collection, use and sale of personal data in direct marketing activities. On 8 July 2011, CMAB published the Amendment Bill in the Gazette setting out the detail provisions of the amendment to the Ordinance.

PCPD's Major Concern on the Amendment Bill

3. In his previous paper (LC Paper No. CB(2)1949/10-11(01)) issued on 31 May 2011, the PCPD has already pointed out the major differences in views between PCPD and the Administration in respect of some key proposals mentioned in the Further Discussion Report. The present paper will concentrate on the practical implementation issues arising from the new provisions in the Amendment Bill.

Collection and Use of Personal data in Direct Marketing

Delayed Notification

4. The new section 35H (under clause 21) of the Amendment Bill requires

data users to inform data subjects by providing certain written information before using their personal data in direct marketing. Data users will have to provide a response facility to data subjects for them to exercise their opt-out right. Data subjects, who do not respond to the data users' response facility within the prescribed 30-days period will, pursuant to section 35J (2)(b), be deemed not to have opted-out. There are crucial flaws in this proposed regime.

5. While Data Protection Principle ("**DPP**") 1(3) in Schedule 1 of the Ordinance requires the purpose of the use of the data (direct marketing or otherwise) to be made known to the data subject *on or before* collecting the data, the proposed notification arrangement legitimizes the data users to delay informing the data subjects until any time after data collection that the data are to be used for direct marketing purposes. With this delayed approach, the data user's notification can take place at any un-predetermined time after data collection. In addition, it would be incumbent on the data subjects to make specific opt-out requests in response to the notification or else the deeming rule applies. As such, data users are likely to make more use of delayed notification rather than notification on or before data collection. There could be attempts to deliberately delay notification and this possible abuse has not been addressed in the Amendment Bill.

Practical Difficulty in Exercising Opt Out Right

6. There are also conceivable difficulties in coming up with a fair and effective system of delayed notification by the data users. Even though the new section 35H(3) (under clause 21) of the Amendment Bill requires data users to provide data subjects with written information, there is no provision governing how such written information is to be brought to the attention of the data subjects, such as the means of giving written notification and whether written notification has to be sent to the data subjects at their respective last known addresses. Since data users are not required to give notifications on or before collecting the data, they may not have data subjects' update contact particulars when serving the written notifications after data collection. The means of notification may fail for one reason or another. Failure of the data subjects to exercise their opt-out options may be due to non-receipt of the data users' notifications and the application of the deeming rule in the circumstances would be unfair to the data subjects.

7. If a data subject exercises his opt out right subsequent to the prescribed

30-days response period (the new section 35K of the Amendment Bill), the difficulties he faces could well be insurmountable. At this late stage, he may be dealing with the transferee(s) of his personal data rather than the data user making the data transfer. He may not even be able to identify the original data source and tackle the problem at its root. Data subject will have to make opt-out request to each and every data transferee that approaches him.

8. Worse still, the new section 35L(2) (under clause 21) of the Amendment Bill imposes a new restriction on the data subjects *to exercise opt-out only in writing* for the use of their personal data in direct marketing activities when they are approached by data users for the first time. This requirement creates an undue hurdle for data subjects especially if the data users approach them by phone. Currently, there is no restriction imposed under section 34 of the Ordinance to require data subjects to opt out *in writing*.

Sale of Personal Data in Direct Marketing

9. An opt-out approach is proposed for seeking data subjects' consent to sell their personal data. A data user may deem the data subject to have agreed sale of his/her personal data if no opt-out request is received within the prescribed 30-days response period after the data user has issued the written notification which provides an option (through a response facility) for the data subject to object to the sale of his personal data. In a way, such deeming effect will legalize the sale of personal data by data users that they are not otherwise permitted to engage in under the current law. The reason is that in most if not all cases where the data subject is not informed before or at the time of data collection that the data would be sold, sale of data as the purpose of use would fall outside the reasonable expectation of the data subject and therefore not consistent with or directly related to the original purpose of use of the data. In the circumstances, DPP 3 in Schedule 1 of the Ordinance requires the data user to obtain the prescribed consent of the data subject before the data could be sold. Hence, under the current regime, unless the data user receives a positive indication from the data subject, the data user cannot sell the personal data of the data subject. In sum, the current proposal falls short of the strong public expectation revealed in the Octopus incident and represents a retrograde step in tightening up control over the unauthorized sale of personal data by data users.

10. Furthermore, since the relevant provisions governing notification and

opt-out are similar to those relating to collection and use of personal data in direct marketing, the comments made in paragraphs 4 to 7 above apply.

Regulation of Data Processors and Sub-contracting Activities

11. To impose indirect obligation on data users to use contractual or other means to require data processors to comply with the requirements under DPP2(2) (on retention), DPP3 (on use) and DPP4 (on security) in Schedule 1 of the Ordinance, corresponding amendments have been introduced in clause 39(19) and (26) of the Amendment Bill.

12. It is to be noted that each DPP in Schedule 1 of the Ordinance governs different aspects of the data cycle. In particular, DPP3 governs exclusively the use (including disclosure or transfer) of personal data while DPP4 governs security of personal data. The classification and contents of the DPPs mirror the equivalent requirements of international standards such as the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* which are widely adopted in many overseas data protection laws (such as the European Union, Australia and New Zealand). It is however noted in clause 39(26) of the Amendment Bill that the amendment to regulate data processors indirectly on the use of personal data is introduced under DPP4. To achieve consistency with international standards, it is considered more appropriate to introduce this provision with regard to the use of personal data under DPP3.

Enforcement Notice

13. The power of the Privacy Commissioner to serve enforcement notices on data users to remedy the contraventions will be revised by virtue of section 50 (under Clause 27) of the Amendment Bill. The condition that the contraventions in the circumstances will likely to continue or be repeated is no longer required before the Privacy Commissioner may serve enforcement notices. Also, the Privacy Commissioner will be empowered to specify the steps that data users must take (including ceasing any act or practice) to remedy the contraventions (new section 50 (1A)(c)). It is however not entirely clear whether the scope of such steps will be confined to remedy the contravention attributed to the data user's *act or omission* under section 50(1A)(b)(ii). Very often, the cause of contravention may be due to the inadequacy (rather than the absence) of the data user's policy practice, or procedure. Under the existing provision of section 50(iii), the Privacy

Commissioner is vested with the wide power to direct data users to take steps to address such inadequacy for the purpose of remedying the contraventions or *matters occasioning the contraventions*. It is important that the Privacy Commissioner's power will not be eroded as a result of the legislative amendment.

Self-Incrimination

14. The new section 60A(2) (under clause 33) of the Amendment Bill will create practical difficulty and enforcement anomaly. The purpose of section 60A(1) is to create a new exemption for data users from complying with data access request on the ground of self-incrimination in line with the common law right. The proposed section 60A(2) will render information provided in compliance with DPP6 or section 18(1)(b) inadmissible as evidence against the data user for any offence under the Ordinance. However, non-compliance of data access request by data users can be due to many reasons other than on the ground of self-incrimination. For instance, many of such non-compliance cases involve contravention of section 19(1) of the Ordinance where the data user provided a copy of a document pursuant to DPP6 or section 18(1)(b) in purported compliance of a data access request but deliberately conceal or edit some personal data contained in the document which should be provided to the data requestor. If information so provided is rendered inadmissible against data users, it will be extremely difficult (if not impossible) to bring successful prosecution. In such circumstances, the new section 60A(2) will stifle the enforcement and prosecution work on suspected contravention of section 19(1) of the Ordinance.

Concluding remarks

15. The PCPD urges the Administration and the Legislative Council Bills Committee to give due consideration to the views set out above in order to meet the rising public expectation for protecting personal data privacy. Despite the aforesaid differences in view between the PCPD and Administration, the PCPD welcomes the Administration's determination to put forward the majority of the proposals originally suggested by the PCPD in order to enhance personal data protection in Hong Kong.

Office of the Privacy Commissioner for Personal Data
November 2011