Bills Committee on
Personal Data (Privacy) (Amendment) Bill 2011

Use of Personal Data in Direct Marketing and Sale of Personal Data

PURPOSE

This paper sets out the changes we propose to make to the provisions in the Personal Data (Privacy) (Amendment) Bill 2011 ("the Bill") regulating the use of personal data in direct marketing and sale of personal data, drawn up having taken into consideration the views expressed by Members and the Privacy Commissioner for Personal Data ("the PCPD") and our discussions with organisations in the sectors concerned.

DIRECT MARKETING

Proposals in the Bill

2. The Bill includes provisions requiring a data user who intends to use personal data in direct marketing or provide personal data to other persons for use in direct marketing to inform the data subject in writing of the kinds of personal data to be used or provided, the classes of persons to which the data is to be provided, and the classes of marketing subjects. The data user is also required to provide the data subject with a response facility through which the data subject may, without charge from the data user, indicate in writing to the data user whether the data subject objects to the intended use or provision (i.e. opt-out mechanism). Such information and response facility must be presented in a manner that is easily readable and easily understandable.

3. If, after the provision of the information and response facility, the data subject sends a reply to the data user indicating that he does not object, the data user may proceed to use or provide the data for use in direct marketing. The reply has to be in writing, whether or not through the response facility. If no reply indicating objection is sent within 30 days after the information and response facility are given to the data subject or after the data is collected, the data subject will be taken not to object (the "taken not to object if no reply sent within 30 days

arrangement”).

4. A data user who uses personal data in direct marketing or provides personal data to other persons for use in direct marketing without complying with any of the requirements in paragraph 2 above or against the wish of the data subject will be liable, on conviction, to a fine of $500,000 and imprisonment for three years.

5. The Bill further provides that, irrespective of whether a data subject has, within the 30-day response period, sent any written reply to the data user indicating no objection, the data subject may subsequently, at any time, object in writing to the use or provision of his personal data and the data user will then have to cease to use or provide the data subject’s personal data for use in direct marketing. Failure of the data user to do so will be an offence. The penalty will be a fine of $500,000 and imprisonment for three years.

Concerns Expressed

6. On the proposal to adopt the opt-out mechanism for regulating the use and provision of personal data in direct marketing, while the PCPD considers that the ultimate goal should be the adoption of the opt-in mechanism, he noted that it would take time for consumers to adjust to this and that most of the overseas jurisdictions at present adopt the opt-out mechanism. He accepts adoption of the opt-out mechanism for direct marketing for now. However, he has grave concerns about the “taken not to object if no reply sent within 30 days arrangement”. He considers that “no reply” cannot be taken as “no objection” as the notification may not have reached the data subject (because, for example, the data user’s record of the data subject’s address is not up-to-date) or the data subject’s reply to indicate objection (if any) may not have reached the data user. Members share these concerns.

7. The “taken not to object if no reply sent within 30 days arrangement” is intended to cater for situations where the data user did not intend to use or provide the data subject’s personal data to others for use in direct marketing at the time of data collection but only intends to do so after the personal data has been collected. A Member considers that, to address this, a grandfathering arrangement for personal data collected before the entry into force of the new requirements (“pre-existing personal data”) should be introduced, instead of instituting the “taken not to object if no reply sent within 30 days arrangement”. The organisations in the sectors concerned that we have consulted also

consider that if this arrangement has to be withdrawn, pre-existing data should be grandfathered.

8. The PCPD also considers that the requirement that a subsequent indication of objection (see paragraph 5) must be in writing would pose an unnecessary hurdle to the data subject.

Revised Proposals

"Taken not to object if no reply sent within 30 days arrangement"

9. Having regard to the concerns in paragraph 6 above, we propose to withdraw the "taken not to object if no reply sent within 30 days arrangement". Instead, we propose that if a data user did not intend to use or provide a data subject's personal data to others for use in direct marketing at the time of data collection but intends to do so subsequently, he can only do so if he has provided in writing the information and response facility as required in paragraph 2 above (which must be presented in a manner that is easily readable and easily understandable) and received a written reply (whether or not through the response facility) from the data subject indicating that the data subject does not object to the data user doing so. If the data user has not received such a reply from the data subject and uses, or provides the data subject's personal data to others for use, in direct marketing, the data user will be liable, on conviction, to a fine of $500,000 and imprisonment for three years.

Grandfathering

10. On the proposal for a grandfathering arrangement for pre-existing personal data, in fact the Bill already contains a provision on grandfathering, subject to certain conditions. New section 35I(1) provides that, for personal data which a data user has, before the entry into force of the new requirements, used in direct marketing in compliance with the existing requirements under the Personal Data (Privacy) Ordinance ("PDPO"), and which the data user intends to use (but not provide to other persons) in relation to the same marketing subject[1], the new requirements in paragraph 2 above will not apply.

11. Our intention is that the grandfathering arrangement will apply to the same class of marketing subjects. There is a case for such an

[1] Under new section 35A, "marketing subject" means (a) any goods, facility or service offered or advertised; or (b) any purpose for which donations or contributions are solicited.

arrangement as the data subject had been approached previously on such direct marketing activities of the data user, the data subject could have requested the data user to cease had he so wished but he has not done so, and direct marketing activities for the same class of marketing subjects should fall within the data subject's reasonable expectation. However, the current wording of new section 35I(1) does not accurately reflect our intention. We therefore propose to replace "same marketing subject" with "same class of marketing subjects".

12. This "grandfathering" arrangement will not affect data subjects' right to indicate objection at any time. As provided for under new section 35L(2), a data subject may, at any time, require the data user to cease to use his personal data in direct marketing.

Requirement for subsequent indication of objection to be in writing

13. The PCPD considers that the requirement for subsequent indication of objection (see paragraph 5) to be in writing may create an undue hurdle for data subjects. He noted that section 34 of the current PDPO, which provides that data subjects may request data users to cease using their personal data in direct marketing, does not contain such an "in writing" requirement.

14. The proposed "in writing" requirement was aimed to provide greater certainty to both data users and data subjects. Noting that many direct marketing activities are conducted over the phone and this requirement may make it more inconvenient for data subjects to indicate objection to the data user's use of his personal data in direct marketing, we propose to withdraw the "in writing" requirement. In other words, data subjects may require the data user to cease to use his personal data in direct marketing in writing or orally.

15. The Bill provides that a data subject may, when indicating objection subsequently, require the data user to notify the persons to whom personal data of the data subject has been provided to cease to use the data in direct marketing. Under the Bill, this has to be done in writing. We also propose to withdraw this "in writing" requirement. In other words, this may be done in writing or orally.

Other

16. The Bill does not explicitly require data users to state explicitly in the information to be provided to data subjects pursuant to the

requirements in paragraph 2 above that the data user intends to use the data subject's personal data, or provide such data to other persons for use, in direct marketing. For the sake of clarity, we propose to add this requirement to the Bill.

SALE OF PERSONAL DATA

Proposals in the Bill

17. The Bill introduces specific requirements regarding sale of personal data. A data user who intends to sell personal data must, before the sale, inform the data subject in writing of the kinds of personal data to be sold and the classes of persons to which the data is to be sold. The data user is also required to provide the data subject with a response facility through which the data subject may, without charge from the data user, indicate in writing to the data user whether the data subject objects to the intended sale (i.e. opt-out mechanism). Such information and response facility must be presented in a manner that is easily readable and easily understandable.

18. If, after the provision of the information and response facility, the data subject sends a reply to the data user indicating that he does not object to the sale, the data user may proceed to sell the data. The reply has to be in writing, whether or not through the response facility. If no reply indicating objection to the sale is sent by the data subject to the data user within 30 days after the information and response facility are given to the data subject or after the data is collected, the data subject will be taken not to object ("taken not to object if no reply sent within 30 days arrangement").

19. A data user who sells personal data without complying with any of the requirements in paragraph 17 above or against the wish of the data subject will be liable, on conviction, to a fine of $1,000,000 and imprisonment for five years.

20. Irrespective of whether a data subject has, within the 30-day response period, sent any written reply to the data user indicating no objection, the data subject may subsequently, at any time, object in writing to the sale of his personal data and the data user will then have to cease to sell the data subject's personal data. Failure of the data user to do so will be an offence. The penalty will be a fine of $1,000,000 and imprisonment for five years.

Concerns Expressed

21. Similar to the proposed regulatory regime for the use and provision of personal data in direct marketing, Members and the PCPD have reservations on the "taken not to object if no reply sent within 30 days arrangement" in respect of sale of personal data. The PCPD also considers that the adoption of the opt-out mechanism, coupled with the "taken not to object if no reply sent within 30 days arrangement", will not be able to ascertain clearly a data subject's wish regarding the intended sale. He has suggested adopting the opt-in mechanism for sale of personal data instead. Some Members have asked the Administration to consider the issues and concerns raised by the PCPD.

22. The PCPD also considers that the requirement that a subsequent indication of objection (see paragraph 20) must be in writing would pose an unnecessary hurdle to the data subject.

23. Separately, there are also concerns that the definition of "sell"[2] in the Bill is so wide that it may inadvertently catch activities which are generally accepted by, and fall within the reasonable expectation of, data subjects. Some examples are public bodies providing copies of information (which contains personal data) in their registers at a fee, and sale of newspapers and other publications which more often than not contain personal data.

Revised Proposals

"Taken not to object if no reply sent within 30 days arrangement"

24. In view of the concerns expressed, we propose to withdraw the "taken not to object if no reply sent within 30 days arrangement". Instead, we propose that if a data user did not intend to sell a data subject's personal data at the time of data collection but intends to do so subsequently, he can only do so if he has provided in writing the information and response facility as required in paragraph 17 above (which must be presented in a manner that is easily readable and easily understandable) and received a written reply (whether or not through the response facility) from the data subject indicating that the data subject does not object to the sale. If the data user has not received such a reply

[2] Under new section 35A, "sell", in relation to personal data, means to provide the data to a person for gain in money or other property, irrespective of whether (a) the gain is contingent on any condition, or (b) the provider retains possession of the data.

from the data subject and sells the data subject's personal data, the data user will be liable, on conviction, to a fine of $1,000,000 and imprisonment for five years.

25. Under both the revised regulatory regimes for direct marketing and sale of personal data, data users will be required to provide data subjects with an opportunity to indicate objection to the use of their personal data in direct marketing or sale of their personal data. Adopting the same mechanism for the regulatory regimes for direct marketing and sale of personal data would avoid confusion to data users and data subjects, facilitate understanding of the new requirements, and obviate the need for data users to put in place different systems for different activities, thus facilitating compliance. The revised requirement proposed in paragraph 24 above that a data user has to receive a written reply from the data subject indicating that the latter does not object before he can sell the personal data will significantly tighten the regulatory regime. Data subjects will be given an opportunity to indicate whether they object to the sale of their personal data and the written reply will be a clear indication of data subject's wish. The proposed revised regulatory regime will afford adequate protection to data subjects.

Requirement for subsequent indication of objection to be in writing

26. We note the concern that the requirement for a subsequent indication of objection (see paragraph 20) to be in writing may make it more inconvenient for data subjects to indicate objection. We propose to withdraw the "in writing" requirement. In other words, data subjects may require the data user to cease to sell his personal data in writing or orally.

27. The Bill provides that a data subject may, when indicating objection subsequently, require the data user to notify the persons to whom personal data of the data subject has been sold to cease to use the data. Under the Bill, this has to be done in writing. We also propose to withdraw this "in writing" requirement. In other words, this may be done in writing or orally.

Scope of the regulatory regime for sale of personal data

28. The proposed new regulatory regime for sale of personal data is to address community concerns over recent cases of sale of massive

customer personal data by some enterprises to others for direct marketing purposes without explicitly and specifically informing the customers of the sale and seeking their consent. Noting the concerns that the definition of "sell" in the Bill may inadvertently catch activities which are generally accepted by, and fall within the reasonable expectation of, data subjects, we now propose to amend the Bill to confine the proposed regulatory regime to sale of personal data for direct marketing purposes.

Other

29. The Bill does not explicitly require data users to state explicitly in the information to be provided to data subjects pursuant to the requirements in paragraph 17 above that the data user intends to sell the data subject's personal data. For the sake of clarity, we propose to add this requirement to the Bill.

A TIGHTENED REGULATORY REGIME

30. The proposed regulatory regimes for direct marketing and sale of personal data seek to address community concerns over recent cases of sale/transfer of massive personal data by some enterprises to others for direct marketing purposes without explicitly and specifically informing the customers of the sale or transfer, and seeking the customers' consent. They also seek to address the inadequacies of the relevant provisions in the existing PDPO. A table indicating how the proposed new requirements (revised as set out in this paper) address those concerns and inadequacies is at the **Annex**. These requirements, taken together, represent a tightened regulatory regime with stronger deterrent effect, affording better protection to personal data privacy.

Constitutional and Mainland Affairs Bureau
February 2012

Annex

How the proposed requirements address community concerns about use of personal data in direct marketing and sale of personal data

Concerns	Proposed Requirements
Data users not giving explicit and specific information Data users do not explicitly and specifically inform data subjects of the intended use of the data subjects' personal data in direct marketing, provision of the data subjects' personal data to others for use in direct marketing, or sale of the data subjects' personal data for direct marketing.	Data users will be required to inform the data subject <u>in writing</u> of: - their intention to use the data subject's personal data in direct marketing, provide the data subject's personal data to others for use in direct marketing, or sell the data subject's personal data for direct marketing purposes; - the kinds of personal data to be used, provided or sold; - the classes of persons to which the data is to be provided or sold for direct marketing purposes; and - the classes of marketing subjects in relation to which the data is to be used for direct marketing.
Presentation of information When such information is provided, it is usually set out in small print.	Data users will have to present the required information in a manner that is easily readable and easily understandable.
Data subjects not given opportunity to indicate their wish When subscribing for a service, the data subject is often required to provide his	Data users will be required to provide the data subject with a response facility

Concerns	Proposed Requirements
personal data and sign a contract/ subscription form containing provisions on, among other things, the purposes for which the personal data collected is to be used, including use in direct marketing. The data subject is not given the option to indicate objection to the intended use or provision of his personal data to others for use in direct marketing, or sale of his personal data.	through which the data subject may, without charge from the data user, indicate whether the data subject objects to the intended use or provision of his personal data to others for use in direct marketing or sale of his personal data for direct marketing purposes. Data users **have to receive written replies** from data subjects indicating no objection before they can proceed with the use, provision or sale.
Sanctions Contravention of Data Protection Principles 1 or 3 (on collection of personal data and use of personal data respectively) is not a criminal offence and may result only in the issue of an enforcement notice by the PCPD. The maximum penalty for contravening the requirements relating to direct marketing under section 34(1)(ii) of the PDPO [3] is only a fine at Level 3 ($10,000). The sanctions in the existing PDPO are not high enough to provide adequate deterrent effect.	Contravention of the requirements relating to direct marketing will be a criminal offence. The penalty will be a fine of $500,000 and imprisonment for three years. Contravention of the requirements relating to sale of personal data for direct marketing purposes will be a criminal offence. The penalty will be a fine of $1,000,000 and imprisonment for five years .

[3] Section 34 of the PDPO provides that if a data user uses personal data obtained from any source for direct marketing purposes, he must, the first time he so uses the personal data, inform the data subject that the data user is required to cease to so use the data if the data subject so requests. Section 34(1)(ii) provides that, if the data subject requests the data user not to use his personal data for direct marketing purposes, the data user shall cease to so use the data.