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

Responses to Issues raised by the Bills Committee

This paper provides responses to the issues raised at previous Bills Committee meetings and the questions on the proposed new section 14A(3) and the proposed amendments to section 20(1) and (3) raised at the meeting on 13 March 2012.

Issues Raised at Previous Meetings

Section 19

2. At the meeting on 13 December 2011, the following queries relating to section 19 were raised:

(a) whether the penalty for a data user who did not comply with a data access request under the proposed new section 19(1) should be increased, for example, by introducing a daily fine for continued contravention; and

(b) in connection with the proposed new section 19(1)(b), whether a person who did not hold any personal data (and hence was not a data user) would still be bound by the duty to inform the requestor that he/she did not hold the data.

3. Subject to sections 19(2), 20 and 28(5), if a data user fails to comply with a data access request within 40 days after receiving the request, the data user commits an offence and is liable to a fine at level 3. If, after conviction, the data user still fails to comply with the data access request, it would be open for the data subject to make another request for the same piece of personal data. If, subject to sections 19(2), 20 and 28(5), the data user again fails to comply with that request, the data user would be liable to prosecution again.

4. If the data user has contravened Data Protection Principle ("DPP") 6 (on access to personal data), the Privacy Commissioner for Personal Data ("PCPD") may issue an enforcement notice. A data user who contravenes an enforcement notice commits an offence and is liable, on first conviction, to a fine at level 5 and to imprisonment for 2 years, and if the offence continues after the conviction, to a daily penalty of $1,000.

5. The proposed new section 19(1)(b) provides that if a data user does not hold any personal data which is the subject of a data access request, the data user must inform the requestor in writing that the data user does not hold the data. Under section 2 of the Personal Data (Privacy) Ordinance ("PDPO"), the definition of "data user" includes not only persons who hold personal data but also persons who control the collection, holding, processing or use of the data. As long as a person falls under the definition, the person would be required to inform the requestor whether the person holds the data.

Section 59(2)

6. At the meeting on 31 January 2012, the Administration was asked to elaborate the justifications for the proposed new section 59(2), which provides that personal data relating to the identity or location of a data subject is exempt from the provisions of DPP 3 (on use of personal data) if the application of those provisions to the data would be likely to cause serious harm to the physical or mental health of the data subject or any other individual.

7. The proposed new section 59(2) aims to address situations which require the timely provision of identity and location data to facilitate immediate actions to be taken by the relevant parties to prevent serious harm to the physical or mental health of an individual. The proposed exemption was one of the proposals on which we invited public views during the two rounds of public consultation in 2009 and 2010. Of the submissions received which expressed views on this proposal, the majority supported its implementation. There are also similar exemption provisions in the legislation of Australia, New Zealand and Canada as set out at Annex A.

Questions Raised at Meeting on 13 March 2012

Section 14A(3)

8. At the meeting on 13 March 2012, in relation to the proposed new section 14A(3) which allows a data user to refuse to provide any document, record, information or thing or any response to any question as required by the PCPD if he is entitled or obliged under any other Ordinance to do so, the Administration was asked to elaborate the justifications for this provision and specify the other Ordinance(s).

9. A data user is required under section 14 of the PDPO to submit to the

PCPD a return containing the prescribed information set out in Schedule 3 to the PDPO. The proposed new section 14A provides an additional power for the PCPD to require a person to provide any document, record, information or thing or respond to any question, in order to assist the PCPD in verifying the accuracy of the information in data user returns.

10. However, there are secrecy provisions in a number of ordinances. When formulating the secrecy provisions in other relevant ordinances, all relevant factors would have been taken into account. Those secrecy provisions do not put an absolute ban on disclosure of information but invariably allow disclosure under specified circumstances. How wide or narrow the "disclosure leeway" should be has to be decided having regard to the policy objectives of and subject matters dealt with by individual ordinances. For example, section 4 of the Inland Revenue Ordinance (Cap. 112) and section 120 of the Banking Ordinance (Cap. 155) impose stringent secrecy provisions on information obtained under the Ordinances but allow disclosure of the information to the person to whom the information relates. Section 15 of The Ombudsman Ordinance (Cap. 397) permits information obtained in the course of an investigation to be disclosed only for the purposes of, among others, proceedings under the Ordinance or reporting evidence of crimes to ensure, inter alia, that investigations would not be jeopardized. Secrecy provisions reflect the outcome of a balancing exercise in respect of different policy considerations (including personal data protection) and were subject to careful legislative scrutiny before enactment. It is not appropriate for the PCPD's additional power to obtain information under the proposed new section 14A to override the secrecy provisions in other ordinances.

11. Also, it would not be practicable to specify all ordinances under which a person is entitled or obliged to refuse to provide any document, record, information or thing or any response to any question as required by the PCPD. It would be more appropriate to set out the general rule that the PCPD's additional power under the proposed section 14A should be subject to the secrecy provisions in other ordinances.

Section 20(1) and (3)

12. At the meeting on 13 March 2012, the Administration was asked to consider specifying the other ordinances under which a data user is obliged or entitled to refuse to comply with a data access request.

13. The proposed amendments to section 20(1) and (3) are intended to resolve the conflict between the requirement to comply with a data access

request under section 19 on the one hand and the requirement to comply with secrecy provisions in other ordinances on the other. Without these amendments, a data user bound by a statutory duty to maintain secrecy will face a dilemma of either breaching the data access provision of the PDPO or the relevant secrecy provision in another ordinance. At the same time, the PCPD's decision may be challenged if he accepts a data user's compliance with a statutory secrecy requirement or a statutory right to non-disclosure as a ground for refusing a data access request.

14. These proposed amendments were one of the proposals on which we invited public views during the two rounds of consultation in 2009 and 2010. Of the submissions received which expressed views on this proposal, the majority supported its implementation. They agreed with the proposed arrangement and considered that this proposal could save the data user from the dilemma of either contravening the provisions of the PDPO on data access or the relevant secrecy provision in another ordinance.

15. It is worth reiterating that the secrecy provisions in ordinances were subject to careful legislative scrutiny before enactment. The specific secrecy requirements and "disclosure leeway" provided under different secrecy provisions reflect the outcome of a balancing exercise in respect of the policy considerations of and the subject matters dealt with by the ordinances. It would not be practicable to specify all ordinances under which a data user is obliged or entitled to refuse to comply with a data access request. It would be more appropriate to set out the general rule that data access requests should be subject to the secrecy provisions in other ordinances. There are similar provisions in the legislation of Australia and New Zealand (Annex B).

16. The Office of the PCPD advised that they had received complaints of refusal to comply with data access request because of the need to comply with secrecy provisions in other ordinances. However, they are not in a position to disclose further details in view of their duty to maintain secrecy under section 46 of the PDPO.

Constitutional and Mainland Affairs Bureau
Department of Justice
March 2012

Annex A

Provisions in overseas legislation similar to the proposed new section 59(2)

Privacy Act 1988 (Australia)

Schedule 3 – National Privacy Principles

Principle 2 – Use and disclosure

2.1 An organization must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless:

……

(e) the organization reasonably believes that the use or disclosure is necessary to lessen or prevent:

(i) a serious and imminent threat to an individual's life, health or safety; or
(ii) a serious threat to public health or public safety; or

……

Privacy Act 1993 (New Zealand)

Section 6 – Information privacy principles

Principle 10 – Limits on use of personal information

An agency that holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose unless the agency believes, on reasonable grounds:

……

(d) that the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to –

(i) public health or public safety; or

(ii) the life or health of the individual concerned or another individual; or

……

Personal Information Protection and Electronic Documents Act (Canada)

Section 7 – Disclosure without knowledge or consent

(3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is:

……

(e) made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure;

……

Annex B

Provisions in overseas legislation similar to the proposed amendments to section 20(1) and (3)

Privacy Act 1988 (Australia)

Principle 6 of Schedule 3 – Access and correction

6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that:

……

(g) providing access would be unlawful; or

(h) denying access is required or authorised by or under law; or

……

Privacy Act 1993 (New Zealand)

7. Savings

…….

(2) Nothing in principle 6 or principle 11[1] derogates from any provision that is contained in any other Act of Parliament and that —
(a) imposes a prohibition or restriction in relation to the availability of personal information; or
(b) regulates the manner in which personal information may be obtained or made available.

……

[1] Principle 6 is on access to personal information and principle 11 is on limits on disclosure of personal information.