LC Paper No. CB(2)1347/11-12(01)

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

Responses to Issues Raised by the Bills Committee

This paper provides responses to some of the issues raised at previous Bills Committee meetings.

Section 8(1)(g)

2. At the meeting on 7 December 2011, the following queries relating to the proposed amendment to section 8(1)(g) were raised:

(a) whether the proposed amendment was appropriate, as it did not duly reflect the mutual assistance relationship between the Privacy Commissioner for Personal Data ("PCPD") and his counterparts in jurisdictions outside Hong Kong and this was more a power than function; and

(b) whether it was appropriate to use the word "shall", which might give rise to an interpretation that the PCPD had a duty to provide assistance upon request from his counterparts outside Hong Kong and did not have the discretion to decide whether to accede to such requests.

3. The intention is that the PCPD should have the power to, and the discretion to decide whether to, provide assistance to and enlist assistance from his counterparts in jurisdictions outside Hong Kong. On closer examination, the preamble of section 8(2) empowers the PCPD to do all such things as are necessary for, or incidental or conducive to, the better performance of his functions and this already allows mutual assistance, within the ambit of the preamble, between the PCPD and his counterparts in jurisdictions outside Hong Kong. We will move a Committee Stage Amendment ("CSA") to withdraw the proposed amendment to section 8(1)(g).

Section 8(2A)

4. At the meetings on 7 and 13 December 2011, the Administration was asked to provide a written response on the following:

(a) the existing fee-charging policy for the PCPD's services and activities, past examples of the PCPD's fee-charging services and activities, and use of the fees received;

(b) given that it should be the PCPD's priority to devote his Office's resources to the general public rather than individual organisations, the relationship between the PCPD's fee-charging power under the proposed new section 8(2A) and his duty to promote awareness and understanding of, and compliance with, the provisions of the Personal Data (Privacy) Ordinance ("PDPO"), in particular the data protection principles under section 8(1)(c) of the PDPO; and

(c) whether the proposed section 8(2A) should be revised having regard to members' concerns and suggestions.

5. In discharging his functions, the PCPD provides a wide range of promotional and educational activities/services/publications/materials. Those targetted at the general public and educational institutions are provided free of charge. They seek to promote awareness and understanding of the provision of the PDPO, which is one of the functions of the PCPD under section 8(1)(c) of the PDPO. For those targetted at specific sectors or customised to meet the needs of individual organisations, the PCPD will charge a fee based on the cost recovery principle. However, having regard to the PCPD's function under section 8(1)(c) to promote awareness and understanding of, and compliance with, the provisions of the PDPO, the actual fee charged may be reduced taking into account the payer's affordability and the market rates for similar products and services.

6. To illustrate this, the PCPD has recently organised a series of professional workshops tailored to the needs of those dealing with personal data in different work contexts. A consultant was engaged to conduct some of the courses. To recover the consultant's fee, the PCPD would have had to charge a fee of about $500 per participant. Taking into account the market rate for similar courses (about $600 - $800 per participant) and in order not to discourage participation of small and medium sized enterprises, the PCPD eventually charged $450 per participant.

7. The charges received by the PCPD for the provision of promotional or educational activities/services/publications/materials will

be credited to PCPD's Subvention Account which will go towards funding PCPD's activities and services for the public. There is no staff bonus scheme in the PCPD.

8. The PCPD would not arbitrarily impose charges for promotional or educational activities or services. The formulation in the proposed new section 8(2A), modelled on a similar provision in the Sex Discrimination Ordinance (Cap. 480)[1], provides that the PCPD may only impose charges that are reasonable.

Section 14(9)(c)

9. The Personal Data (Privacy) (Amendment) Bill 2011 ("the Bill") proposes to amend section 14(9) to read:

> "It is hereby declared that-
>
> ….
>
> (c) subsection (4) shall not operate to prejudice the generality of section 67(4)(c)."

10. At the meeting on 13 December 2011, the following query relating to section 14(9)(c) was raised: whether the reference to section 67(4)(c) therein should be replaced by section 67(4).

11. Section 14(4) imposes the requirement to submit a data user return in the specified form to the PCPD while section 67(4)(c) requires that the submission of the specified form to the PCPD must be in the manner, if any, specified in the form.

12. There is no conflict between section 14(4) and section 67(4)(c) and thus the declaration in section 14(9)(c) is not necessary. It is of note that other sections which refer to "specified form" (for example, sections 15(6), 16(2) and 31(1)(a)) do not contain the "without prejudice" clause as in section 14(9)(c). We will move a CSA to delete section 14(9)(c).

Sections 14A and 15

13. At the meeting on 13 December 2011, the following queries relating to sections 14A and 15 were raised:

[1] Section 65(2) of the Sex Discrimination Ordinance reads "The Commission may impose reasonable charges for educational or other facilities or services made available by it."

(a) whether the information contained in the data user return under the proposed new section 14A(1) should include accompanying documents and notice of changes;

(b) which are the provisions “under this or any other Ordinance” referred to in the proposed new section 14A(3) on the basis of which a person was entitled or obliged to refuse to comply with a notice served under the proposed new section 14A(1);

(c) whether the knowing or reckless provision of “corrected” but still false or misleading information in the data user return in accordance with the proposed new section 14A(4) should also be subject to the sanction under section 14A(6);

(d) whether corresponding amendments to section 15 (including section 15(1) and (2)), in view of the proposed new section 14A under which there might be information provided subsequent to the original return, should be made; and

(e) whether “prescribed form” in section 15(3) was different from “specified form” in section 14(4).

14. On paragraph 13 (a), (c) and (d) above, it is our intention that:

(a) the PCPD should have the authority to require any persons as specified in section 14A(2) to provide any document, record, information or thing for the purpose of verifying the accuracy of information, including information in a data user return submitted under section 14(4), subsequent changes notified to the PCPD under section 14(8), or supplementary information or corrections provided under the proposed new section 14A(5);

(b) any person who knowingly or recklessly provides any information in a data user return, whether it is the return first submitted or a subsequently updated/corrected return, which is false or misleading in a material particular is liable on conviction to a fine at level 3 and to imprisonment for 6 months; and

(c) the register of data users kept and maintained under section 15 should include any updates/corrections made as appropriate subsequent to the submission of the original data user return.

We will move a CSA to make the above clear.

15. On paragraph 13(b) above, the proposed new section 14A provides the PCPD the authority to require production of information for the purpose of verifying the accuracy of information in a data user return. At the same time, a number of other ordinances contain provisions (for example, section 4 of Inland Revenue Ordinance (Cap. 112), section 4 of Monetary Statistics Ordinance (Cap. 356) and section 31 of Hong Kong Export Credit Insurance Corporation Ordinance (Cap. 1115)) requiring certain information to be kept secret. Section 14A(3) was proposed to allow a person to refuse to provide any document, record, information or thing etc which he is entitled or obliged under any other ordinance to do so. However, the words “this or” in the proposed new section 14A(3) are unnecessary and we will move a CSA to delete them.

16. On paragraph 13(e) above, the “specified form” in section 14(4) refers to the data user return containing the prescribed information that a data user is required to submit annually. The “prescribed form” in section 15(3) refers to the notice containing the prescribed information which the PCPD may require a data user to supply in order to keep and maintain the register of data users. Although the forms referred to in sections 14(4) and 15(3) govern different situations, they both relate to provision of information in connection with the data user return scheme. For consistency’s sake, we will move a CSA to amend “prescribed form” in section 15(3) to “specified form”.

Section 20

17. At the meeting on 3 January 2012, the Administration was asked to:

(a) in connection with the proposed amendment to section 20(1)(c) under which a data user “shall refuse to comply with a data access request ...… in any other case, if compliance with the request is for the time being prohibited under this or any other Ordinance”, specify the other Ordinance(s), if any; and

(b) in connection with the proposed new section 20(3)(ea) under which “the data user is entitled under this or any other Ordinance not to disclose the personal data which is the subject of the request”, specify the other Ordinance(s), if any;

(c) provide the justifications for the proposed new section 20(5), clarify the relevant provisions concerning discovery and inspection referred to therein and whether the High Court's inherent jurisdiction is unable to deal with the situations under section 20(5), identify the possible problems arising form the absence of section 20(5), and confirm whether the Magistrate Ordinance (Cap. 227) and a magistrate are not to be covered by the definitions of "relevant Ordinance" and "specified body" under the proposed new section 20(6).

18. There are secrecy provisions in a number of ordinances. The purpose of the proposed amendment to section 20(1)(c) and the proposed new section 20(3)(ea) is to make clear that while data subject should have the right to access his own personal data, such right should be subject to the secrecy concerns in other ordinances. When formulating the secrecy provisions in other relevant ordinances, all relevant factors including not only the need to preserve secrecy, but also the need to respect the data subject's right to access his own personal data would have been taken into account. For this reason, some ordinances such as the Inland Revenue Ordinance (Cap. 112) impose a duty of secrecy on officials concerned but allow the data subject to access his own personal data, whereas some other ordinances such as the Sex Discrimination Ordinance (Cap. 480) do not allow such access (since for example, in the case of the Sex Discrimination Ordinance, allowing a complainee to access information relating to him might compromise the integrity and confidentiality of the investigation process).

19. It would not be practicable to specify all ordinances under which compliance with a data access request is prohibited or refusal to comply with a data access request is allowed. It would be more appropriate to set out the general rule that the right for a data subject to access his own personal data should be subject to the non-disclosure/secrecy requirements in other ordinances.

20. On paragraph 17(c) above, under the PDPO, a data subject may lodge a complaint with the PCPD against a data user who failed to comply with the data subject's request to access his own personal data. In the course of an investigation, the PCPD may request production of the requested data and may keep a copy of the requested data for record. After the PCPD has made a decision, the aggrieved party (who may be the data subject) may lodge an appeal with the Administrative Appeals Board ("AAB").

21. Under the Administrative Appeals Board Ordinance (Cap. 442), save for documents for which a claim to privilege against disclosure is made, the PCPD as the respondent is obliged to give description of every document that is in his possession or under his control which relates to the appeal (including the document which contains the requested data) to the AAB Secretary, the appellant and the person(s) bound by the decision appealed against. The standing instruction made by the AAB would also normally require the PCPD to serve on the AAB, the appellant and the person(s) bound by the decision appealed against a copy of every document in the possession or under the control of the PCPD and this can include a copy of the requested data.

22. Similarly, the High Court Ordinance (Cap. 4) and the District Court Ordinance (Cap. 336) both contain provisions (e.g. sections 41 and 42 of the High Court Ordinance and sections 47A and 47B of the District Court Ordinance) under which the court may make orders for discovery and inspection of documents relevant to the action before the court. The Rules of the High Court (Cap. 4A) and The Rules of the District Court (Cap. 336H) also contain provisions that permit discovery of documents without court order.

23. In proceedings relating to non-compliance with a data access request under the PDPO, the disclosure mentioned above would enable the data subject to obtain the requested data before the AAB or the court rules on the case. This would mean that the data subject will already have had access to the requested data, even if the AAB or the court ultimately rules that the data user’s refusal to comply with the data access request is lawful.

24. In order to forestall the disclosure of document containing the data in dispute to the data subject and other parties bound by the decision of the AAB or the court by way of discovery or otherwise before the AAB or the court determines in favour of the appellant, we have proposed to add the new section 20(5).

25. The proposed new section 20(5) applies to proceedings before a magistrate but it is not necessary to include “Magistrates Ordinance” in the definition of “relevant Ordinance” as the Magistrates Ordinance does not contain any provisions relating to discovery and inspection.

Section 22(4)

26. At the meeting on 3 January 2012, the Administration was asked, in connection with the proposed repositioning of the existing section 64(2) to the proposed new section 22(4):

(a) to consider whether it is too harsh to impose across the board a criminal penalty on the supply of false or misleading information in a material particular in a data correction request and whether the penalty is necessary as there is no corresponding offence when the data is first supplied;

(b) to advise whether the supply of information has to be in writing;

(c) to specify the relevant section under which the data correction request under the proposed new section 22(4) is made; and

(d) to provide the precedents, if any, for the enforcement of the existing section 64(2).

27. The offence in the proposed new section 22(4) is not a new offence. This is a repositioning of the existing section 64(2). Section 22(4) (or the existing section 64(2)) provides that a person who, in a data correction request, supplies any information which is false or misleading in a material particular <u>for the purpose of</u> having the personal data corrected as indicated in the request commits an offence.

28. There can be various reasons why an individual may choose not to provide accurate information about himself. For example, an individual may provide fake data when opening an email account in order to conceal his identity for the purpose of privacy protection. Currently, provision of inaccurate personal data is not an offence and it will be going overboard to impose criminal liability on data subjects for providing inaccurate personal data to data users generally.

29. The supply of false or misleading information for making a data correction request is different. Since the data subject would need to take the initiative to make a data access request and subsequently a data correction request, there must be a specific purpose in mind for the data subject to seek correction of the data. It should also be noted that the data concerned may not be provided by the data subject in the first place but may be obtained by the data user from other sources. In this regard, criminal penalty would become necessary if the data subject knowingly

or recklessly supplies false or misleading information for the purpose of having the data user concerned comply with the request.

30. It should be noted that there is the element of "knowingly" or "recklessly" in the existing section 64(2). This will be retained in the proposed new section 22(4). The prosecution is required to prove that the defendant knows, or is reckless as to whether, the information supplied is false or misleading in a material particular. As the threshold required for committing this offence is high, we consider it appropriate to impose a criminal penalty if it can be proved that the data subject knows, or is reckless as to whether, the information supplied is false or misleading in a material particular.

31. A data correction request or the supply of information need not be in writing but if the request is not in writing, the data user may refuse to comply with the data correction request (see section 24(3)(a)).

32. Data correction request is already defined under section 2 to mean a request under section 22(1). According to information provided by the PCPD, no prosecution has been instituted under the existing section 64(2) as at the date of this response.

Section 31

33. At the meeting on 3 January 2012, the Administration was asked to consider the suggestion to add "knowingly or recklessly" to the proposed new section 31(4) to require that there must be mens rea for the offence of supplying false or misleading information by a data user in a matching procedure request made under section 31(1).

34. The offence in section 31(4) is not a new offence. This is a repositioning of the existing section 64(4). Section 31(4) (or the existing section 64(4)) provides that the supply of any information which is false or misleading in a material particular <u>for the purpose of</u> obtaining the PCPD's consent to the carrying out of a matching procedure is an offence. Under the existing formulation, the prosecution is required to prove that the defendant knows that, or is reckless as to whether, the information supplied is false or misleading in a material particular. The element of "knowingly or recklessly" is already inherent in the proposed new section 31(4) (i.e. the existing section 64(4)).

Section 32(5)

35. At the meeting on 3 January 2012, the Administration was asked to consider, in relation to the proposed new section 32(5), whether the penalty should include a penalty of imprisonment.

36. The offence and penalty in section 32(5) are not new. This is a repositioning of the existing section 64(5). According to information provided by the PCPD, the PCPD has not received any complaint relating to data users' conduct of matching procedures. In the light of this, we do not intend to increase the existing penalty level as set out in the proposed new section 32(5) (i.e. the existing section 64(5)).

Section 46

37. At the meeting on 3 January 2012, the Administration was asked to advise on/consider the following:

(a) the safeguards for personal data in cross-border commercial transactions;

(b) the scope of co-operation and relevant agreements between the PCPD and the authorities in jurisdictions outside Hong Kong and the safeguards for personal data exchanged during the cooperation;

(c) whether the definition of "relevant function" in the proposed new section 46(8), in relation to an authority of a place outside Hong Kong to which the PCPD may disclose matters is too broad; and

(d) the policy justifications for the proposed new sections 46(7) to (9), such as empowering the PCPD to disclose matters to other authorities in jurisdictions outside Hong Kong in the absence of consent in writing by a data subject to whom the matter related.

38. Under the existing section 46(1), the PCPD and every prescribed officer are subject to a statutory duty to maintain secrecy in respect of all matters that come to their actual knowledge in handling complaints, investigations and inspections. This secrecy duty survives after completion of an investigation or inspection unless the matter is included in a report published pursuant to section 46(3). This restricts the ability of

the PCPD to cooperate with privacy enforcement authorities in other jurisdictions.

39. Under international and regional enforcement cooperation arrangements, authorities handling privacy matters may seek assistance or make referrals regarding information privacy investigations and enforcement matters that involve each other's jurisdictions. Assistance could involve cooperating on enforcement action, sharing information about an organization or a matter being investigated, collecting evidence in relation to privacy investigations, or transferring an information privacy complaint to another privacy enforcement agency for investigation, where appropriate. For example, during an investigation, a privacy enforcement authority in one place may seek the assistance of an authority in another place, if certain evidence of the alleged privacy violation is located in the jurisdiction of the other authority. Parallel or joint investigation may also be necessary in dealing with a case which involves a single incident in one place which affects individuals in other jurisdictions or where a global organisation engages in practices at multiple locations that affect personal data privacy. If privacy enforcement authorities are unable to share information, this will duplicate each other's work and multiply the effort required to obtain the necessary information and evidence. It is therefore important that the PCPD is given the discretion to share information about potential or existing investigations or enforcement actions to facilitate possible coordination with other privacy enforcement authorities.

40. The PCPD has joined the Asia Pacific Economic Cooperation Cross-border Privacy Enforcement Arrangement[2] since August 2010. The PCPD is also a member of the International Conference of Data Protection and Privacy Commissioners ("ICDPPC")[3].

41. Members has raised the concern that the definition of "relevant function" in the proposed new section 46(8) may be too broad. We will move a CSA to amend the proposed new section 46(7)(c) and (8) to restrict disclosure to an authority of a place outside Hong Kong if the disclosure will enable or assist that authority in performing its functions of investigation into suspected contravention of, or in enforcement of, any

---

[2] http://aimp.apec.org/Documents/2011/ECSG/DPS2/11_ecsg_dps2_010.pdf

[3] The resolutions of the ICDPPC's 29th and 33rd Conferences on cross-border privacy investigation and enforcement (at http://www.privacyconference2011.org/htmls/adoptedResolutions/2007_Montreal/2007_M2.pdf and http://www.privacyconference2011.org/htmls/adoptedResolutions/2011_Mexico/2011_GA_RES_001_%20Intl_Priv_Enforc_ENG.pdf) are relevant.

law which is substantially similar to, or serves the same purposes as, the PDPO or if such disclosure is necessary for the proper performance of the PCPD's functions or the proper exercise of the PCPD's powers under the PDPO.

Section 50A

42. At the meeting on 9 January 2012, the Administration was asked, in relation to the proposed new section 50A:

(a) to elaborate on the reasons for the different penalties under the proposed new section 50A(3) and (1)(b) and consider whether they should be aligned; and

(b) to provide information on whether any person has been imprisoned for contravention of enforcement notice.

43. Under the existing PDPO, a data user who contravenes an enforcement notice commits an offence and is liable on conviction to a fine at level 5 and to imprisonment for two years, and in the case of a continuing offence, to a daily penalty of $1,000. Under the existing PDPO, a data user who has complied with an enforcement notice and then intentionally does the same act or makes the same omission which occasioned the issue of the enforcement notice is not liable to criminal proceedings. The PCPD can only issue an enforcement notice again. The proposed new section 50A(3) plugs this potential loophole by making such act an offence. Since this is akin to first time contravention of an enforcement notice, a penalty same as that for first time contravention of an enforcement notice is proposed.

44. The proposed new section 50A(1)(b), on the other hand, proposes to impose for repeated contraventions of enforcement notices a higher penalty than that for first time contravention. This is because repeated contraventions are more culpable.

45. According to the information provided by the PCPD, so far there have been three conviction cases for contravention of enforcement notice. One offender was fined $1,000 while the other two were fined $5,000.

Section 50B

46. At the meeting on 9 January 2012, the Administration was asked to clarify who the "any other person" referred to in the proposed section 50B(1)(c) is.

47. The proposed section 50B is not a new provision. This is a repositioning of the existing section 64(9). Pursuant to section 9(1), the PCPD may employ such persons, and engage, other than by way of employment, such technical and professional persons as he thinks fit to assist him in the performance of his functions, and the exercise of his powers. "Any other person" is included in the proposed section 50B (or the existing section 64(9)) so that not only the PCPD, but also other persons who assist him in the performance of his functions and the exercise of his powers under Part VII of the PDPO (on inspections, complaints and investigations) would be covered.

48. To delineate more clearly the coverage of "any other person", we will move a CSA to replace "any other person" by "any prescribed officer". "Prescribed officer" is already defined under section 2 to mean a person employed or engaged by the PCPD under section 9(1).

Section 59A

49. At the meeting on 31 January 2012, the following queries relating to the proposed new section 59A were raised:

(a) whether there would be any guidelines or training for officers in the Hong Kong Police Force and the Customs and Excise Department in respect of the application of the exemption in the proposed new section 59A(1); and

(b) the rationale for the defence provision in the proposed new section 59A(2) (and also the proposed new section 63C(2)).

50. The purpose of the proposed new section 59A is to facilitate parents/guardians to provide proper parental care and guardianship. Given the prevalence and hidden nature of drug abuse nowadays, notifying the parents/guardians of such matters would boost preventive efforts, and facilitate early identification of hidden problems and intervention for treatment and rehabilitation to prevent the problems from further deteriorating. The exemption will only be invoked by an officer

not lower than the rank of Station Sergeant (or equivalent rank) if he is satisfied that all three conditions set out in the proposed new section 59A(1) are met. More detailed guidelines and training materials for reference of police and customs officers will be prepared as necessary.

51. The proposed new section 59A(2) is intended to provide for a defence for persons who acted out of good faith. Having reconsidered this in the light of Members' views, we will withdraw the proposed new section 59A(2) (as well as that in the proposed new section 63C(2)).

Section 63D

52. At the meeting on 31 January 2012, the Administration was asked to consider improving the drafting of the proposed new section 63D to make clear that the proposed exemption from Data Protection Principle ("DPP") 3 would not apply when the records containing personal data transferred to the Government Records Service ("GRS") for archive purposes were made available for public access.

53. Section 63D(1) provides that "*personal data contained in records of historical, research, educational or cultural interest that are transferred to the Government Records Service for archive purposes is exempt from the provisions of data protection principle 3.*" The words "*…… contained in records … … for archive purposes*" qualify the personal data. The data must be contained in records of historical, research, educational or cultural interest which are transferred to the GRS for archive purposes. The proposed exemption will apply only if the records are for archive purposes. The proposed section 63D(2)(b) specifically stipulates that "archive" does not include accessing the record from the repository in which it is retained for purposes unrelated to the management or preservation of the record. When the records are used for public access in the GRS, they no longer constitute records that are transferred to the GRS for archive purposes and the personal data contained in the records will not be exempt from DPP 3. The existing drafting has already made this clear.

Section 64

54. At the meeting on 7 February 2012, a Member asked whether an imprisonment sentence should be introduced for the offence in the proposed section 64(1) in order to achieve greater deterrent effect.

55. The proposed section 64(1) is not a new provision. This is a repositioning of the existing section 64(10) (with some drafting changes). The proposed section 64(1) stipulates that a data user who contravenes any requirement, other than those set out in the proposed section 64(2), commits an offence and is liable on conviction to a fine at level 3. The proposed section 64(2)(b) covers contraventions of a more serious nature for which higher penalties (including imprisonment sentence where appropriate) are proposed. The penalty for the contraventions in the proposed section 64(1) is considered appropriate. Moreover, for these contraventions, apart from instituting proceedings against the data user, it is also open for the PCPD to 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.

Data Protection Principles 2(3) and 4(2) in Schedule 1

56. At the meeting on 7 February 2012, the Administration was asked to consider amending the reference to "手段" in the Chinese version of the proposed new subsection (3) of DPP 2 and the proposed new subsection (2) of DPP 4. We will move a CSA to replace "手段" by "方法" in the subsections.

57. We will separately provide responses to other issues raised by the Bills Committee.

Constitutional and Mainland Affairs Bureau
Department of Justice
March 2012