立法會
Legislative Council

LC Paper No. CB(2)1553/10-11(05)

Ref : CB2/PL/CA

Panel on Constitutional Affairs

Updated background brief prepared by the Legislative Council Secretariat for the meeting on 18 April 2011

Review of the Personal Data (Privacy) Ordinance

Purpose

This paper provides background information on the review of the Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO") and summarizes the major issues raised by the Panel on Constitutional Affairs ("the CA Panel") concerning the review and the legislative proposals in the Report on Public Consultation on Review of the Personal Data (Privacy) Ordinance ("the Consultation Report") issued by the Administration in October 2010.

Background

2. The Law Reform Commission ("LRC") published a report entitled "Reform of the Law relating to the Protection of Personal Data" in August 1994. Most of the recommendations in the report had been implemented with the enactment of PDPO on 3 August 1995. PDPO was brought into force on 20 December 1996.

3. The Privacy Commissioner for Personal Data ("PCPD") appointed by the Chief Executive is conferred with the responsibility for monitoring, supervising and promoting compliance with the Ordinance. To enable PCPD to carry out his statutory functions, the Office of the Privacy Commissioner for Personal Data ("the Office of PCPD") was established in 1996. The Office of PCPD investigates suspected breaches of PDPO and issues enforcement notices ("ENs") to data users as appropriate.

The Ordinance

4. PDPO protects the privacy of individuals in relation to personal data only. The Ordinance covers any data relating directly or indirectly to a living

individual ("data subject"), from which it is practicable to ascertain the identity of the individual and which are in a form in which access or processing is practicable. It applies to any person ("data user") who controls the collection, holding, processing or use of personal data. Data users must follow the fair information practices stipulated in the six data protection principles ("DPPs") in Schedule 1 to PDPO in relation to the purpose and manner of data collection, accuracy and duration of data retention, use of personal data, security of personal data, availability of data information, and access to personal data.

5. A data user in breach of an EN is liable to criminal sanction which carries a penalty of a fine at Level 5 (at present $25,001 to $50,000) and imprisonment for two years.

6. PDPO gives rights to data subjects. They have the right to confirm with data users whether their personal data are held, to obtain a copy of such data, and to have personal data corrected. Data subjects whose personal data have been compromised may seek damages through civil proceedings; however, there are no statutory provisions or resources at present for PCPD to assist data subjects in claiming damages.

7. PDPO shall not apply if the data pertains to an individual whose identity is unknown, or there is no intention to identify that individual. The Ordinance also provides specific exemptions from its requirements as follows -

(a) a broad exemption from the provisions of the Ordinance for personal data held for domestic or recreational purposes;

(b) exemptions from the requirements on subject access for certain employment related personal data; and

(c) exemptions from the subject access and use limitation requirements of the Ordinance where their application is likely to prejudice certain competing public or social interests, such as security, defence and international relations, prevention or detection of crime, assessment or collection of any tax or duty, news activities, and health.

Review of PDPO

8. The Office of PCPD formed an internal Ordinance Review Working Group in June 2006 to assess the adequacy of the Ordinance in protecting personal data privacy of individuals. At its meeting on 4 July 2008, the Panel on Home Affairs ("the HA Panel") discussed the progress of the review with the

Constitutional and Mainland Affairs Bureau and the former PCPD. According to the Administration, a major objective of the comprehensive review of PDPO was to examine whether the existing provisions of the Ordinance still afforded adequate protection to personal data having regard to developments, including advancement in technology.

9. With effect from the 2008-2009 legislative session, the policy area of personal data protection has been placed under the purview of the CA Panel. On 28 August 2009, the Administration, with the support of the Office of PCPD, issued the Consultation Document on Review of the PDPO ("the Consultation Document") to invite public views on the proposals to amend the Ordinance. According to the Administration, conduct of the review was guided by the following factors -

(a) the right of individual to privacy was not absolute which must be balanced against other rights and public and social interests;

(b) balance was needed between safeguarding personal data privacy and facilitating continued development of information and communications technology;

(c) any changes to the privacy law should not undermine Hong Kong's competitiveness and economic efficiency as an international city;

(d) there was a need to avoid putting onerous burden on business operations and individual data users;

(e) due account should be given to local situations;

(f) PDPO should remain flexible and relevant in spite of technological change;

(g) legislative intervention might not always be the most effective way and personal data privacy protection might be achieved by administrative measures in certain circumstances, and

(h) consensus in the community about the privacy issues was important.

10. At the special meeting of the CA Panel held on 11 September 2009, the Administration and the former PCPD briefed members on the major proposals in the Consultation Document and the major areas of difference in views between the Administration and the Office of PCPD. After the end of the

public consultation exercise on 30 November 2009, the Administration published the Consultation Report in October 2010. The proposals to be taken forward by the Administration and those the Administration had considered but decided not to pursue as extracted from the Consultation Report are in **Appendix I** and **Appendix II** respectively.

11. According to the Administration, the legislative proposals in the Consultation Report were drawn up in the light of the views received during the public consultation exercise and the recent developments including the Octopus Incident. In the Incident, Octopus cardholders' personal data collected under the Octopus Rewards Programme were passed to third parties by Octopus Rewards Limited for direct marketing purpose causing wide public concerns over the handling of personal data by enterprises and the inadequacies in the existing legislation for the protection of personal data.

12. Members may wish to refer to the background brief prepared by the Legislative Council ("LegCo") Secretariat (LC Paper No.CB(2)37/10-11(03)) for the meeting of the CA Panel on 18 October 2010 for details on related issues raised by other Panels since the First LegCo.

Major issues raised by the CA Panel

13. Apart from the discussion on the Consultation Document at its special meeting on 11 September 2009, the CA Panel discussed with the Administration and the incumbent PCPD the legislative proposals in the Consultation Report at its meetings held on 18 October, 15 November, 20 November and 20 December 2010 respectively. The Panel also received views from the public at the special meeting on 20 November 2010.

14. The major issues raised by members of the CA Panel at the above meetings are summarized below.

<u>Enforcement powers of PCPD</u>

15. Some members expressed concern that the Administration did not propose in the Consultation Report to grant criminal investigation and prosecution power to PCPD. These members considered that PCPD was not granted adequate power to enhance protection of personal data in the light of serious contraventions of PDPO in recent years and sought explanation from the Administration on the reason for not taking forward PCPD's proposal of granting him such powers.

16. While some other members expressed support for strengthening the powers of PCPD, including his powers to conduct investigations, they considered that vesting enforcement, criminal investigation and prosecution powers in a single body was against the principle of natural justice and might lead to inadequate checks and balances. They opined that strong justifications would be required for concentrating criminal investigation and prosecution powers in a single body in a specific domains as the existing practice of vesting in separate authorities the powers of criminal investigation, prosecution and judging on criminal cases had been functioning well.

17. The Administration explained its position on the proposals relating to the enforcement of power of PCPD as follows -

(a) under the Basic Law ("BL"), the control of criminal prosecutions was vested in Department of Justice ("DoJ"). Although it would not be inconsistent with BL to confer prosecution power on PCPD if the relevant legislation expressly stated that the prosecutions to be brought thereunder were without prejudice to the powers of the Secretary for Justice in relation to prosecution of criminal offences, the policy assessment was that strong justifications would be required for the prerogative of initiating criminal prosecution to be delegated in specific domains;

(b) under the existing arrangements, the power to conduct criminal investigation, prosecute and give ruling on criminal cases were vested with three separate authorities, namely, the Police, DoJ and the Judiciary respectively, in order to ensure a fair trial and judicial independence. The Administration considered that the existing arrangement had been functioning well and should not be changed lightly;

(c) the appropriate body to determine compensation under PDPO had been thoroughly discussed in the LRC's Report on Reform of the Law Relating to the Protection of Personal Data published in August 1994. It was the LRC's view at that time that conferring power on a data protection authority to award compensation would vest in a single authority an undesirable combination of enforcement and punitive functions and recommended that PCPD's role should be limited to determining whether there had been a breach of DPPs;

(d) under the existing PDPO, PCPD could issue ENs in cases where contravention of DDPs were involved. PCPD was also granted

the power to request the relevant data user to provide information and enter premises for the purposes of an investigation. If necessary, PCPD could, pursuant to a warrant issued by a magistrate under section 43 of PDPO, exercise his power to enter premises to conduct investigation without serving notice to the relevant data user. The Administration considered that PCPD could continue to exercise his investigation power available under the existing framework of PDPO; and

(e) on enhancing the sanctioning powers of PCPD, the Administration had proposed to empower PCPD to provide legal advice and assistance to an aggrieved data subject to institute legal proceedings against a data user to seek compensation under section 66 of PDPO. Since PCPD would be empowered to provide such service, it would give rise to conflict of interest if PCPD was also empowered to conduct criminal investigation into contravention of PDPO by a data user. The Administration considered that PCPD should put more emphasis on its education and complaint handling works as an advocate for privacy protection.

18. On members' queries on whether the Police had sufficient resources and expertise to conduct criminal investigation into cases involving contravention of PDPO referred by the Office of PCPD, the Administration assured members that the Police had substantial experience in criminal investigation and attached great importance to handling cases of privacy contravention referred by the Office of PCPD. The Administration further advised that the Police had issued guidelines to frontline officers setting out relevant procedures in handling these cases. A designated officer at Senior Superintendent level in every police region would handle the referred cases in person and assign them to appropriate crime investigation unit for investigation. During the investigation, the Police would in general consult DoJ and if necessary, also seek professional advice from PCPD.

19. PCPD, however, considered that the recent serious contraventions of PDPO and unauthorized sale of personal data had reflected the inadequacy of the enforcement powers of PCPD. The proposal of giving PCPD criminal investigation and prosecution powers could meet the public expectation for enhancing deterrent measures against serious contravention of PDPO. PCPD opined that his team had the knowledge and experience to perform these roles efficiently and effectively, while the discretion of whether or not to prosecute would still vest with the Secretary of Justice. PCPD also took the view that with the expertise and first hand information on a case, his Office could act expeditiously to deal with any suspected offence. Granting independent

prosecution power to PCPD would also help prevent conflict of interest where the Police or other government departments were involved in the case as data user.

20. At the Council meeting on 6 April 2011, Dr Margaret NG raised a written question on the low prosecution of complaint cases related to suspected contravention of PDPO referred by the Office of PCPD to the Police. The question raised by Dr NG and the reply of the Secretary for Constitutional and Mainland Affairs are in **Appendix III**.

Collection, use and sale of personal data

21. Some members considered that as the intrusion of privacy was a serious matter and any resulting harm might not be remediable, any serious contravention of PDPO should be made a criminal offence subject to immediate prosecution in order to enhance deterrent effect. They were concerned that under the existing PDPO, PCPD could only serve an EN on a data user in case of non-compliance with a DPP and it was only upon the issuance of EN and the failure to comply with the directions in the EN that an offence would be committed. Hence, some enterprises which had contravened DPPs therefore did not need to bear any legal consequences provided that they had subsequently complied with the EN.

22. The Administration explained that it noted the concerns of the community that the provisions in the existing legislation were not specific enough to afford adequate protection to personal data privacy. In this regard, the Administration proposed to introduce in PDPO additional specific requirements on data users who intended to use (including transfer) the personal data collected for direct marketing purposes. Under the Administration's proposal, the data user's Personal Information Collection Statement ("PICS") should be reasonably specific about the intended direct marketing activities (whether by the data user himself/herself or the transferee(s)), the classes of persons to whom the data could be transferred for direct marketing purposes and the kinds of data to be transferred for direct marketing purposes.

23. The Administration proposed that a two-step approach would be adopted to regulate collection and use of personal data for direct marketing purposes as well as unauthorized sale of personal data by a data user. While non-compliance with any of the additional specific requirements for collection and use of personal data in direct marketing would be subject to issuance of an EN, it would be a criminal offence if a data user did not comply with such requirements and subsequently used the personal data for direct marketing purposes. Similarly, non-compliance with any of the new requirements for sale of personal data by a data user would be subject to issuance of an EN. It

would be a criminal offence if the new requirements were not complied with and there was subsequent sale of personal data to another person by a data user for a monetary or in kind gain or against the wish of the data subject.

24. Some members cautioned that the Administration should differentiate between sale of personal data by enterprises to others for direct marketing and collection of personal data for its own direct marketing purpose. While the Administration should combat unauthorized use of personal data for monetary gains, it should be mindful of the fact that it was a common business practice for enterprises such as insurance and telecommunication companies to collect the personal data of their clients for its own direct marketing activity and such practice was widely accepted by the public provided that the personal data would be destroyed after use.

25. The Administration assured members that any regulatory measures over the collection and use of personal data in direct marketing would carry sufficient clarity to facilitate compliance by the industries concerned. The principle was that even though personal data was collected with the prescribed consent of the data subject, the data user could not use such personal data for purposes beyond the original purpose of collection.

"Opt-in" and "opt-out" mechanism for collection and use of personal data

26. The Administration proposed to require the data user, on or before collecting personal data, to provide an option for the applicant to choose not to agree to ("opt-out" mechanism) the use (including transfer) of his/her personal data for any of the intended direct marketing activities or the transfer of the data to any class of transferees. For the sale of personal data, the Administration invited public views on whether the data subject should be provided with an opportunity to indicate his/her agreement to ("opt-in" mechanism) or his/her disagreement with ("opt-out" mechanism) the sale. The Administration also considered it not appropriate to introduce a territory-wide "Do-not-call" register against direct marketing activities.

27. Some members expressed strong support for adopting an "opt-out" mechanism on the grounds that it could facilitate business developments, had been adopted by most western countries, and the Administration had already proposed to introduce additional specific requirements to strengthen the regulation over the collection and use of personal data in direct marketing as well as the sale of personal data. They opined that the crux of the issue was to ensure that personal data were used for the intended purposes for which the data were collected and that data users should have the obligation to stipulate clear provisions for data subjects to indicate their choice.

28. Some other members were of the view that adopting an "opt-out" mechanism did not afford adequate safeguards to the personal data as explicit consent of consumer was not required. They also considered that enterprises which had collected consumers' personal data through bundled consent to the terms and conditions of the contract for goods or services should also be required to seek explicit consent from consumers again for further use of their personal data.

29. The Administration stressed that it had proposed to impose additional specific requirements on data users for the collection and use of personal data for direct marketing, as well as for the sale of personal data. These requirements would be applied irrespective of which mechanism to be adopted. If an "opt-out" mechanism was adopted, the Administration would make reference to the existing "Do-not-call" registers compiled by the Office of the Telecommunications Authority under the Unsolicited Electronic Message Ordinance (Cap. 593) with a view to further strengthening the protection of personal data of consumers. The Administration would consider carefully the views of the community to decide on the mechanism to be adopted with a view to striking a balance between safeguarding the personal data privacy of the public and facilitating business operations.

30. PCPD said that while he maintained the view that an "opt-in" mechanism should be the ideal for the protection on personal data privacy because consumers had the right of self-determination on the use of their personal data, he was well aware of the concerns of relevant industries about the adoption of an "opt-in" mechanism. He suggested that interim arrangements, such as a central "Do-not-call" register on person-to-person telemarketing, could be introduced as an "opt-out" means at an initial stage to regulate the use of personal data for making unsolicited promotion calls.

Civil claim for compensation and provision of legal assistance to data subjects under PDPO

31. In response to members' enquiry about the civil liabilities imposed on persons who leaked personal data of another person, the Administration advised that under the existing law, a data subject who suffered damage by reason of a contravention of a requirement under PDPO was given the opportunity to seek compensation from the data user for that damage. In order to create greater deterrent effect on acts or practices which intruded into personal data privacy, the Administration proposed in the Consultation Report to empower PCPD to provide legal assistance to an aggrieved data subject to institute legal proceedings to seek compensation under section 66 of PDPO. Additional

resources would also be allocated to the Office of PCPD to render such service. The Administration, however, decided not to pursue PCPD's recommendations to empower PCPD to award compensation to aggrieved data subjects, or to impose monetary penalty on serious contravention of DPPs.

32. Some members expressed support for the proposal of providing legal assistance to aggrieved data subjects. They further suggested that a fund similar to the Consumer Legal Action Fund of the Consumer Council should be set up to give aggrieved data subjects greater access to legal remedies by providing financial support and legal assistance. They considered that PCPD should also be given the power to mediate complaints.

Data security and protection of privacy on the Internet

33. Some members expressed concern about the misuse and unauthorized use of personal data on the Internet which had aroused widespread public concern and enquired whether legal liability would be imposed on a third party who had intruded into personal data privacy and caused damage to a data subject by disseminating his/her personal data on the Internet.

34. The Administration advised that it proposed making it an offence if a person obtained personal data without the consent of the data user and disclosed the personal data so obtained for profits or malicious purposes. The proposal did not seek to impose criminal liabilities on data users for accidental leakage of personal data not resulting in substantial harm. The proposal was couched in specific terms in order not to catch those who had disseminated personal data unintentionally.

35. Some members were of the view that the Administration should review the definition of "personal data" in light of the development of technology having regard to the Yahoo case in which the IP address of a journalist who was an email user of "Yahoo! China" residing in the People's Republic of China was disclosed by "Yahoo! Holdings (Hong Kong) Limited" leading to his arrest and conviction of the offence of illegally providing state secrets to foreign entities. They were concerned that if a narrow interpretation of "personal data" was adopted, other information such as the data transaction record of internet users which could be used to ascertain the identity of an individual might also be disclosed by internet service providers in the absence of any deterrent measure.

36. The Administration explained that in accordance with the definition under PDPO, personal data referred to any data relating directly or indirectly to a living individual from which it was practicable to ascertain the identity of the individual and which were in a form in which access or processing was

practicable. The Administration held the view that the IP address per se should not amount to personal data within the definition of PDPO. It was pointed out that when dealing with the complaint lodged against the email service provider for infringing PDPO by disclosure of an email subscriber's personal data, the Administrative Appeals Board also concluded the same. This view was also shared by the general public as indicated by the views received during the public consultation exercise. Regarding the data protection on the Internet, the Administration advised that if an IP address was used in conjunction with other identifying particulars of an individual, those data had already been afforded protection under the existing PDPO.

Implementation of section 33 of PDPO

37. Some members considered that section 33 of PDPO, the only provision which had not commenced operation, should be brought into operation as soon as practicable to prohibit the transfer of data by data users to another territory where comparable privacy protection was lacking. Some other members, however, took the view that it would not be practical and feasible to regulate data processing outside Hong Kong having regard to the prevalence of cross-boundary data transfer activities in recent years. They opined that careful re-assessment of the enforceability of the provision would be warranted.

38. The Administration responded that as implementing section 33 would have significant implications on data transfer activities of various sectors of the community, the Administration needed to consult stakeholders to assess the readiness of the community for the operation of section 33. As data users could transfer personal data under section 33 to places with legislation substantially similar to, or served the same purposes as PDPO, PCPD would also need time to specify such places before the provision coming into operation. PCPD advised that he had embarked on the preparation work and provided relevant background information on the privacy protection regime in overseas countries for the Administration's consideration. He would further provide supplementary information as requested by the Administration during the discussion on the implementation of section 33 of PDPO.

Application of PDPO to offices set up by the Liaison Office of the Central People's Government ("CPG")

39. Some members expressed dissatisfaction that after over 10 years since the establishment of the Hong Kong Special Administrative Region ("HKSAR"), the Administration was unable to tell unequivocally whether PDPO applied to the CPG offices in the territory and urged the Administration to expedite its liaison with CPG.

40. The Administration responded that CPG offices in HKSAR had the duty to comply with the provisions of BL. Since the passage of the Adaptation of Laws Ordinance in April 2009, the application of four more Ordinances had been extended to CPG offices in HKSAR. The Administration was working on the extension of the applicability of other Ordinances to CPG offices and would continue with its best effort in this aspect. The current review of PDPO, however, would not cover its application to CPG offices.

41. A summary setting out the views expressed by deputations, PCPD and members at the special meeting of the CA Panel on 20 November 2010 in respect of these major issues is in **Appendix IV**.

Recent development

42. It is the Administration's plan to introduce the relevant bill into LegCo in the first half of 2011. The Administration is scheduled to update the CA Panel on the outcome of the review of PDPO and the legislative proposals at its meeting on 18 April 2011.

Relevant papers

43. A list of the relevant papers available on the LegCo website is in **Appendix V.**

Council Business Division 2
Legislative Council Secretariat
14 April 2011

Summary of Proposals

(A) Proposals to be Taken Forward

Direct Marketing and Related Matters

Proposal (1) : Collection and Use of Personal Data in Direct Marketing

1. To raise the penalty for contravention of the requirement in section 34(1)(b)(ii) of the Personal Data (Privacy) Ordinance ("PDPO") (Cap. 486) (i.e. if the data subject requests the data user not to use his/her personal data for direct marketing purposes, the data user shall cease to so use the data) from a fine at Level 3 ($10,000) to a fine of $500,000 and imprisonment for three years.

2. To introduce in the PDPO the following additional specific requirements on data users who intend to use (including transfer) the personal data collected for direct marketing purposes :

   (a) the data user's Personal Information Collection Statement ("PICS") should be reasonably specific about the intended marketing activities (whether by the data user himself/herself or the transferee(s)), the classes of persons to whom the data may be transferred for direct marketing purposes and the kinds of data to be transferred for direct marketing purposes;

   (b) the presentation of the information in (a) above in the data user's PICS should be understandable and reasonably readable by the general public; and

   (c) the data user should, on or before collecting the personal data, provide an option for the data subject to choose (e.g. by ticking a checkbox) not to agree to the use (including transfer) of his/her personal data for any of the intended direct marketing activities or the transfer of the data to any class of transferees.

3. Non-compliance with any of the requirements in paragraph 2 above

will be subject to the issue of an enforcement notice by the Privacy Commissioner for Personal Data ("PCPD")[Note].

4. The PCPD to revise the guidance note on the collection and use of personal data for direct marketing or replace it with a Code of Practice to provide practical guidance on the new requirements in paragraph 2, and to launch a publicity and public education programme to promote understanding of the new requirements.

5. A data user commits an offence and is liable on conviction to a fine of $500,000 and imprisonment for three years if he/she:

(a) does not comply with any of the requirements in paragraph 2 and subsequently uses (including "transfers") the personal data for direct marketing purposes; or

(b) complies with those requirements but uses (including "transfers") the personal data collected for a direct marketing activity or transfer the data to a class of transferees to which the data subject has indicated disagreement; or

(c) (i) uses (including "transfers") the personal data collected for a direct marketing activity;

(ii) transfers for direct marketing purposes the data to a class of persons; or

(iii) transfers for direct marketing purposes a kind of personal data

not covered in the PICS.

Proposal (2) : Unauthorised Sale of Personal Data by Data User

6. To introduce the following requirements and offence:

(a) if a data user is to sell personal data (whether collected from the data subject direct by the data user or obtained from

---

Note As currently provided for under the PDPO, if a data user contravenes a requirement under the PDPO, the PCPD may issue an enforcement notice to direct the data user to take specified remedial steps within a specified period. If the data user contravenes the enforcement notice, he/she commits an offence under section 64(7), and is liable on conviction to a fine at Level 5 ($50,000) and imprisonment for two years, and in the case of a continuing offence, to a daily penalty of $1,000.

another source) to another person for a monetary or in kind gain, the data user should, before doing so, inform the data subject in writing of the kinds of personal data to be sold and to whom the personal data will be sold;

(b) the presentation of the notice to provide the data subject with the information in (a) above should be understandable and reasonably readable by the general public;

(c) the data user should provide the data subject with an opportunity to indicate whether he/she agrees ("opt-in model") to or disagrees ("opt-out model") with the sale; and

(d) it will be an offence for a data user to sell personal data to another person for a monetary or in kind gain without complying with the requirements in (a) to (c) above or against the wish of the data subject.

7. Non-compliance with any of the requirements in (a) to (c) above will be subject to the issue of an enforcement notice by the PCPD.

8. We welcome public views on the penalty for the offence in (d) above. For reference, section 58(1) of the Unsolicited Electronic Messages Ordinance ("UEMO") (Cap. 593) provides that a person to whom an unsubscribe request is sent shall not use any information obtained thereby other than for the purpose of complying with the relevant requirements (including the requirement to comply with the unsubscribe request). A person who contravenes section 58(1) commits an offence and is liable on summary conviction to a fine at Level 6 ($100,000). A person who knowingly contravenes section 58(1) commits an offence and is liable upon conviction on indictment to a fine of $1,000,000 and imprisonment for five years.

Proposal (3): Disclosure for Profits or Malicious Purposes of Personal Data Obtained without the Data User's Consent

9. To make it an offence for a person who discloses for profits or malicious purposes personal data which he obtained from a data user without the latter's consent.

10. A possible formulation is to define "malicious purposes" as "with a view to gain for oneself or another, or with an intent to cause loss, which includes injury to feelings, to another".

11. To set the penalty at the same level as that for the offence proposed paragraph 6(d).

Proposal (4) : Excluding Social Services from the Definition of "Direct Marketing"

12. To amend section 34 of the PDPO to exclude from the definition of "direct marketing" the offering of social services and facilities by social workers to individuals in need of such services and facilities.

Data Security

Proposal (5) : Regulation of Data Processors and Sub-contracting Activities

13. To require a data user to use contractual or other means to ensure that its data processors and sub-contractors, whether within Hong Kong or offshore, comply with the requirements under the PDPO. Contravention will be subject to the issue of an enforcement notice by the PCPD.

14. The Office of the Privacy Commissioner for Personal Data, Hong Kong ("Office of the PCPD") to step up publicity and education in relation to sub-contracted data processing, and issue codes of practice or guidelines as and when necessary to provide practical guidelines on the terms and conditions to be included in a contract between the data user and its data processor.

Proposal (6) : Personal Data Security Breach Notification

15. To start with a voluntary personal data security breach notification system, under which organisations would notify the PCPD and affected individuals when a breach of data security leads to the leakage of personal data, so that we can adjust the detailed arrangements, if necessary, having regard to actual operational experience and assessment on the impact of leakage notification, with a view to making the system reasonable and practicable.

16. The Office of the PCPD to undertake promotional and educational initiatives to raise awareness of the guidance note on this subject issued by it, promote adoption of a privacy breach notification system by data users voluntarily and assist data users to make appropriate notifications.

Statutory Powers and Functions of the PCPD

Proposal (7) : Legal Assistance to Data Subjects under Section 66

17. To empower the PCPD to provide legal assistance to an aggrieved data subject who intends to institute legal proceedings against a data user to seek compensation under section 66 of the PDPO.

Proposal (8) : Circumstances for Issue of an Enforcement Notice

18. To amend the circumstances under which the PCPD may, following the completion of an investigation, issue an enforcement notice to a data user so that an enforcement notice may be issued in situations where the data user has contravened a requirement under the PDPO, irrespective of whether there is evidence to show that the contravention will likely be repeated. In deciding whether to serve an enforcement notice, the PCPD still has to follow the existing requirement to consider whether the contravention has caused or is likely to cause damage or distress to the data subject.

Proposal (9) : Clarifying Power to Direct Remedial Steps in an Enforcement Notice

19. To specify in the PDPO that, when the remedial actions directed by the PCPD in an enforcement notice to be taken within the specified period include desisting from doing a certain act or engaging in a certain practice, the data user should desist from doing so even after the expiration of the specified period.

Proposal (10) : Removing the Time Limit to Discontinue an Investigation

20. To remove the 45-day time limit within which the PCPD has to notify the complainant if the PCPD refuses to continue an investigation.

Proposal (11) : Additional Grounds for Refusing to Investigate

21. To include "the primary cause of the complaint is not related to personal data privacy" in section 39(2) of the PDPO as an additional ground for the PCPD to refuse to carry out or continue an investigation.

Proposal (12) : Relieving the PCPD's Obligation to Notify the Complainant who has Withdrawn his Complaint of Investigation Result

22. To remove the obligation of the PCPD to inform the complainant of the PCPD's investigation result and the related matters under section 47(3) of the PDPO where the complainant has withdrawn his complaint.

Proposal (13) : PCPD to Serve an Enforcement Notice together with the Result of Investigation

23. To amend section 47 of the PDPO to allow the PCPD to serve an enforcement notice on the relevant data user at the same time when he notifies the relevant parties of the investigation result.

Proposal (14) : PCPD to Disclose Information in the Performance of Functions

24. To allow the PCPD and his prescribed officers to disclose information reasonably necessary for the proper performance of their functions and exercise of their powers.

Proposal (15) : Immunity for the PCPD and his Prescribed Officers from being Personally Liable to Lawsuit

25. To stipulate in the PDPO that the PCPD and his prescribed officers would not be held personally liable for any civil liability for any act done or omission made in good faith in the exercise or purported exercise of the PCPD's functions and powers under the PDPO.

Proposal (16) : Power to Impose Charges for Educational and Promotional Activities

26. To expressly provide the PCPD with power to impose reasonable charges for undertaking educational or promotional activities or services.

Proposal (17) : Power to Obtain Information to Verify a Data User Return

27. To empower the PCPD to obtain information from any person in order to verify the information in a data user return filed under section 14 of the PDPO.

Offences and Sanctions

Proposal (18) : Repeated Contravention of a Data Protection Principle on Same Facts

28. To make it an offence for a data user who, having complied with the directions in an enforcement notice to the satisfaction of the PCPD, subsequently intentionally does the same act or engages in the same practice for which the PCPD had previously issued an enforcement notice.

29. The penalty should be the same as that for breaching an enforcement notice, i.e. a fine at Level 5 ($50,000) and imprisonment for two years.

Proposal (19) : Repeated Non-compliance with Enforcement Notice

30. To impose heavier penalty on data users for repeated non-compliance with enforcement notice, i.e. a fine at Level 6 ($100,000) and in the case of a continuing offence, a daily fine of $2,000, while the term of imprisonment would remain at two years, the same as that for first-time non-compliance with enforcement notice.

Rights of Data Subjects

Proposal (20) : Third Party to Give Prescribed Consent to Change of Use of Personal Data

31. To empower a specified third party to give consent to the change of use of personal data of certain classes of data subjects when it is in their best interests to do so. The specified third parties include, where the individual is a minor, a person who has parental responsibility for the minor, and where the individual is incapable of managing his own affairs, a person who has been appointed by a court to manage those affairs.

Proposal (21) : Access to Personal Data in Dispute

32. To add a provision to prohibit the disclosure of document containing the data in dispute to the data requestor and other parties bound by the decision of Administrative Appeals Board ("AAB"), the court or magistrate by way of disclosure or otherwise before the AAB, the court or magistrate determines in favour of the applicant.

Rights and Obligations of Data Users

Proposal (22) : Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation

33. To add a provision to the PDPO so that a data user can refuse to comply with a data access request where the data user is obliged or entitled under any other ordinances not to disclose the personal data.

Proposal (23) : Response to Data Access Requests in Writing and within 40 Days

34. To require a data user to inform a requestor in writing in 40 days if he does not hold the requested personal data. As regards the handling of data access requests in respect of criminal conviction records by the Police, if the requestor has a clear record, the Police will be exempt from complying with the requirement to reply in writing, though it will still be required to make a verbal response within 40 days.

Proposal (24) : Contact Information about the Individual who Receives Data Access or Correction Requests

35. To amend Data Protection Principle ("DPP") 1(3) to permit a data user to provide the job title or the name of the individual to whom data access or correction requests may be made.

Proposal (25) : Erasure of Personal Data

36. To amend the PDPO to the effect that the duty to erase personal data would be regarded as having been complied with, if a data user can prove that he has taken all reasonably practicable steps to erase obsolete personal data.

Proposal (26) : Duty to Prevent Loss of Personal Data

37. To amend DPP 4 to make it explicit that a data user is required to take all reasonably practicable steps to prevent the loss of personal data.

Introducing New Exemptions

Proposal (27) : Transfer of Personal Data in Business Mergers or Acquisition

38. To grant an exemption from DPP 3 for the transfer or disclosure of personal data in merger, acquisition or transfer of businesses subject to certain conditions. To prevent abuse of the exemption and possible harm to data subjects, we propose to impose a fine at Level 5 ($50,000) and imprisonment for two years for contravention of the requirements on the retention and restriction on the use of the personal data concerned.

Proposal (28) : Provision of Identity and Location Data on Health Grounds

39. To broaden the scope of application of the exemption under section 59 of the PDPO to cover personal data relating to the identity and location of the data subject on health grounds.

Proposal (29) : Handling Personal Data in Emergency Situations

40. To exempt the law enforcement agencies ("LEAs"), rescue and relief agencies, and individuals and organisations holding relevant personal data from DPP 1(3) and DPP 3 to:

(a) identify individuals who are or may reasonably be suspected to be involved in an accident or other life-threatening situations;

(b) inform family members of the individuals under (a) of the latter's involvement in the accident, etc; and

(c) generally to facilitate the provision of rescue or relief services to the individuals under (a).

Proposal (30) : Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship

41. To grant an exemption from DPP 3 for personal data of minors under the following conditions :

(a) the transfer or disclosure of the data to the parents or guardians of the minor is to facilitate the latter to better discharge their responsibility to exercise proper care and guardianship, and is in the best interests of the minor; and

(b) the data are held by LEAs and are to be transferred or disclosed by LEAs to the parents or guardians of the minor.

Proposal (31) : Use of Personal Data Required or Authorised by Law or Related to Legal Proceedings

42. To create an exemption from DPP 3 for use of personal data required or authorised by or under law, by court orders, or related to any legal proceedings in Hong Kong or otherwise for establishing, exercising or defending legal rights.

Proposal (32) : Transfer of Records for Archival Purpose

43. To create an exemption from DPP 3 for the transfer of records containing personal data of historical, research, educational or

cultural interests to the Government Records Service ("GRS") for archival purpose.

Proposal (33) : Refusal to Comply with a Data Access Request on Ground of Self-Incrimination

44. To create a new exemption for data users from complying with a data access request on the ground of self-incrimination.

Proposal (34) : Exemption for Personal Data Held by the Court or Judicial Officer

45. To add a new provision to the PDPO so that the PDPO shall not apply to personal data held by the court or judicial officer in the course of the exercise of judicial functions.

Miscellaneous Proposed Amendments

Proposal (35) : Definition of Crime under Section 58

46. To add a definition of "crime" in order to clarify the scope of the application of section 58 of the PDPO, which provides that personal data used for the purposes of the prevention or detection of crime are exempt from DPP 3.

Proposal (36) : Expanding the Definition of "Relevant Person"

47. To expand the definition of "relevant person" under section 2 of the PDPO to include the guardians of data subjects with mental incapacity, who are appointed under sections 44A, 59O or 59Q of the Mental Health Ordinance (Cap. 136), so that they may lodge complaints and make data access and data correction requests on behalf of the data subjects concerned.

Proposal (37) : Extending the Time Limit for Laying Information for Prosecution

48. To extend the time limit for laying information for prosecution of an offence under the PDPO from six months to two years from the date of commission of the offence.

(B) Proposals NOT to be Taken Forward

Sensitive Personal Data

Proposal (38) : Sensitive Personal Data

49. Not to pursue the proposal to subject sensitive personal data (particularly biometric data) to more stringent regulation such as prohibiting the collection, holding, processing and use of such data except under specific circumstances.

50. Instead, we propose that:

(a) the Office of the PCPD should step up promotion and education and, where necessary, issue codes of practice or guidelines to suggest best practices on the handling and use of sensitive personal data in general, such as biometric data and health record; and

(b) the Office of the PCPD should continue to discuss with the information technology sector possible measures to enhance the protection of biometric data.

Statutory Powers and Functions of the PCPD

Proposal (39) : Granting Criminal Investigation and Prosecution Power to the PCPD

51. Not to pursue the proposal to confer the PCPD with the power to carry out criminal investigations and prosecutions. We consider it important to retain the existing arrangement, under which the Police conducts criminal investigation and Department of Justice undertakes prosecution, in order to maintain checks and balances.

Proposal (40) : Empowering the PCPD to Award Compensation to Aggrieved Data Subjects

52. Not to pursue the proposal to empower the PCPD to determine the amount of compensation to a data subject who suffers damage by reason of a contravention of a requirement under the PDPO by a data user. We do not consider it desirable to vest in a single authority both enforcement and punitive functions. The data

subjects concerned can seek compensation through the court as provided for under section 66 of the PDPO.

Offences and Sanctions

Proposal (41) : Making Contravention of a Data Protection Principle an Offence

53. Not to pursue the proposal to make contravention of a DPP an offence.

Proposal (42) : Imposing Monetary Penalty on Serious Contravention of Data Protection Principles

54. Not to pursue the proposal to empower the PCPD to require data users to pay monetary penalty for serious contravention of DPPs. We consider that it would be more appropriate to make serious contravention a criminal offence.

Access to Personal Data

Proposal (43) : Parents' Right to Access Personal Data of Minors

55. Not to pursue the proposal to permit a data user to refuse a data access request made by a "relevant person" (i.e. a person who has parental responsibility for the minor) on behalf of a minor in order to protect the interests of minors.

Proposal (44) : Fee Charging for Handling Data Access Requests

56. Not to pursue the proposal that, for the purpose of imposition of a fee for complying with a data access request, a fee schedule should be provided in the PDPO and a data user should be required not to charge fees in excess of the prescribed maximum as set out in the said fee schedule.

Others

57. Not to pursue the proposals in Annex 2 to the consultation document on the Review of the Personal Data (Privacy) Ordinance ("the consultation document"), which we had indicated in the consultation document our intention not to pursue.

Appendix III

Press Releases

LCQ2: Enforcement of the Personal Data (Privacy) Ordinance
****

Following is a question by Dr Hon Margaret Ng and a written reply by the Secretary for Constitutional and Mainland Affairs, Mr Stephen Lam, in the Legislative Council today (April 6):

Question:

According to the Year Ender 2010 released earlier by the Office of the Privacy Commissioner for Personal Data ("PCPD"), 1 179 complaint cases related to suspected contravention of the Personal Data (Privacy) Ordinance (Cap. 486) ("the Ordinance") were received by PCPD in 2010, but only 12 of these cases were referred to the Police for consideration of prosecution. Among the cases referred to the Police, prosecution was instituted for only one case so far (the offender was convicted by the court), prosecution would not be instituted for seven cases, and the remaining four are still being followed up. There have been comments that the aforesaid rather low prosecution and conviction figures may give an impression to the public that "the law is laid aside and unused". In this connection, will the Government inform this Council:

(a) whether it knows why PCPD did not make any referral to the Police for a great majority of these complaint cases, and why prosecution has not been instituted by the Police in a majority of the cases referred to them; and

(b) whether the authorities will refine the prosecution policy relating to the Ordinance with a view to enhancing enforcement against contravention of the Ordinance; if they will, of the details?

Reply:

President,

My reply to the two parts of the question is as follows:

(a) The Office of the Privacy Commissioner for Personal Data (PCPD) completed 1 076 complaint cases in 2010. Amongst these, 928 cases involved allegations on contravention of data protection principles (DPPs), which did not constitute any criminal offence. One of them involved contravention of an enforcement notice and was referred to the Police for further investigation. The remaining 148 cases involved alleged offences under the Personal Data (Privacy) Ordinance (the Ordinance) (Cap. 486). Of these 148 cases, after considering the information collected, the Privacy Commissioner for Personal Data (Privacy Commissioner) referred 11 of them to the Police for further investigation. Details of the remaining 137 cases are as follow:

* Three cases in which the parties complained against took remedial action by signing an undertaking;

* One case in which no contravention of the requirements under the Ordinance was found after investigation;

* Nine cases were outside the purview of the Ordinance;

* 61 cases were found to have no prima facie evidence;

* Four cases were withdrawn by the complainants during enquiries;

* Five cases were found to be unsubstantiated after enquiries with the parties being complained against;

* 51 cases in which the complainants had not responded to enquiries from the PCPD; and

* Three cases were resolved through mediation.

Of the 12 cases referred by the Privacy Commissioner to the Police for further investigation, one was withdrawn by the complainant and three cases are still under investigation. For the eight remaining cases, two cases resulted in conviction. The other six cases were not prosecuted by the Department of Justice (DoJ) because of insufficient evidence after considering factors such as the actual circumstances of the relevant acts and the evidence collected.

(b) The Statement of Prosecution Policy and Practice is applicable to the prosecutions instituted under the Ordinance. The reasonable prospect of conviction will be taken into account by the DoJ when considering prosecution. If there is a reasonable prospect of conviction, further assessment will be made on whether prosecution is in the public interest. The existing prosecution policy is based on sound legal principles to ensure that criminal justice can be administered to all in a fair and just manner.

Instituting prosecution is one of the aspects of law enforcement. According to the Ordinance, the Privacy Commissioner may also handle the complaints received through other enforcement actions (for example issuing warning letters or enforcement notices to the parties complained against). As such, the effectiveness of the enforcement of the Ordinance cannot be simply measured by referring to the number of prosecution cases.

Ends/Wednesday, April 6, 2011
Issued at HKT 12:32

NNNN

Appendix IV

Panel on Constitutional Affairs

Report on Public Consultation on Review of the Personal Data (Privacy) Ordinance ("the Consultation Report")

Summary of the views and suggestions of the deputations attending the special meeting on 20 November 2010

* proposal to be taken forward by the Administration
\# proposal not to be taken forward by the Administration

No.	Deputation [LC Paper No. of submission]	Views and suggestions
1.	Hong Kong Human Rights Monitor	*<u>Proposal 1: Collection and use of personal data in direct marketing</u> (a) An opt-in mechanism should be adopted for affording better protection to consumers as data users will need to state clearly the purposes for the collection and use of the data for the consideration of data subjects. (b) A blanket refusal to adopt the opt-in mechanism is not justified as there can be different modes to implement the opt-in mechanism which does not have to be applied across-the-board. *<u>Proposal 6: Personal data security breach notification</u> (c) A mandatory personal data security breach notification system should apply to government organizations/public bodies and a voluntary system to the private sector.

No.	Deputation [LC Paper No. of submission]	Views and suggestions
		#Proposal 39: Granting criminal investigation and prosecution power to the Privacy Commissioner for Personal Data ("PCPD") (d) A statutory obligation should be imposed on government organizations and pubic bodies to provide professional/technical assistance to PCPD in order to strengthen his investigation power. Prohibition against transfer of personal data to place outside Hong Kong except in specified circumstances (e) Section 33 of the Personal Data (Privacy) Ordinance (Cap.486) ("PDPO") should be brought into operation to prohibit the transfer of data by data users to another territory where comparable privacy protection is lacking. Register of data users (f) PCPD should compile the Register of Data Users as soon as possible. Application of PDPO (g) The Administration should clarify whether PDPO will be applicable to the offices set up by the Central People's Government ("CPG") in the Hong Kong Special Administrative Region ("HKSAR").

No.	Deputation [LC Paper No. of submission]	Views and suggestions
2.	Young Democratic Alliance for Betterment of Hong Kong [LC Paper No. CB(2)443/10-11(01)]	*Proposal 2: Unauthorized sale of personal data by data user *Proposal 3: Disclosure for profits or malicious purposes of personal data obtained without the data user's consent (a) Serious contravention of PDPO such as unauthorized sale of personal data or disclosure for profits or malicious purposes of personal data obtained without the data user's consent should be made a criminal offence. However, defense provisions should be included in the legislation such as public interest defense, and the intent of the accused for profit-making or malicious purposes should be proved for the constitution of an offence. *Proposal 7: Legal assistance to data subjects under section 66 of PDPO (b) PCPD should be empowered to provide legal assistance to an aggrieved data subject to institute legal proceedings to seek compensation under section 66 of PDPO. #Proposal 39: Granting criminal investigation and prosecution Power to PCPD (c) PCPD should not be conferred with the power to carry out criminal investigations and prosecutions as it is important to retain the existing arrangement under which the criminal investigation and prosecution are undertaken respectively by the Police and Department of Justice in order to maintain checks and balances.
3.	Democratic Party [LC Paper No. CB(2)379/10-11(01)]	*Proposal 1: Collection and use of personal data in direct marketing (a) An "opt-in" mechanism should be adopted for direct marketing activities.

No.	Deputation [LC Paper No. of submission]	Views and suggestions
		(b) When carrying out direct marketing activities, data users should have the responsibility to inform data subjects of the source of their personal data. (c) A central Do-not-call register on person-to-person telemarketing should be established. *<u>Proposal 6: Personal data security breach notification</u> (d) A mandatory personal data security breach notification system should be put in place in phases which can be applied initially to high-risk private business sectors such as the finance and banking sector which involve frequent use of personal data. The application can be further extended to other business sectors having regard to the level of sensitivity of personal data involved. *<u>Proposal 7: Legal assistance to data subjects under section 66 of PDPO</u> (e) PCPD should be empowered to provide legal assistance to an aggrieved data subject to institute legal proceedings to seek compensation under section 66 of PDPO but mediation services should be provided to solve the disputes before resorting to legal actions. #<u>Proposal 38: Sensitive personal data</u> (f) The Administration should discuss with the information technology industry with a view to classifying sensitive personal data into different categories and drawing up clear guidance for more stringent regulation.

No.	Deputation [LC Paper No. of submission]	Views and suggestions
		#Proposal 39: Granting criminal investigation and prosecution power to PCPD (g) PCPD should be granted criminal investigation power. Internet protocol ("IP") address as personal data (h) IP address per se should be regarded as personal data within the definition of PDPO. Prohibition against transfer of personal data to place outside Hong Kong except in specified circumstances (i) Section 33 of PDPO should be brought into operation to prohibit the transfer of data by data users to another territory where comparable privacy protection is lacking. Register of data users (j) PCPD should compile register of data users as soon as possible to cover the Octopus Holdings Limited and other industries such as banking, insurance, and telecommunications and require these registered data users to submit returns (on their collection, usage and disclosure of personal data) and compliance reports. Application of PDPO (k) The Administration should clarify whether PDPO will be applicable to the CPG offices in HKSAR.

No.	Deputation [LC Paper No. of submission]	Views and suggestions
4.	Society for Community Organization [LC Paper No. CB(2)317/10-11(01)]	*<u>Proposal 1: Collection and use of personal data in direct marketing</u> (a) An opt-in mechanism should be adopted for direct marketing activities. (b) The direct marketing industry should come up with proposals on how the personal data of consumers could be better protected if an "opt-out" mechanism is to be adopted. *<u>Proposal 6: Personal data security breach notification</u> (c) A mandatory personal data security breach notification system should be applied to government organizations at an initial stage and be further extended to other business sectors in phases. #<u>Proposal 38: Sensitive personal data</u> (d) The Administration should introduce a categorization system for sensitive personal data with a view to affording better protection of such data. #<u>Proposal 39: Granting criminal investigation and prosecution Power to PCPD</u> (e) Criminal investigation and prosecution power should be granted to PCPD. #<u>Proposal 43: Parents' right to access personal data of minors</u> (f) Data users should be given the legal right to deny access to the personal data of the minors by their parents or guardians in order to strike a balance between respecting parents' right to have reasonable access to the personal data of their children and respecting the children's privacy right.

No.	Deputation [LC Paper No. of submission]	Views and suggestions
		#Proposal 44: Fee charging for handling data access requests (g) A data user should be required not to charge fees in excess of the prescribed maximum as set out in the fee schedule to be provided in PDPO for the purpose of imposition of a fee for complying with a data access request. Prohibition against transfer of personal data to place outside Hong Kong except in specified circumstances (h) Section 33 of PDPO should be brought into operation to prohibit the transfer of data by data users to another territory where comparable privacy protection is lacking.
5.	Hong Kong Direct Marketing Association [LC Paper No. CB(2)317/10-11(02)]	*Proposal 1: Collection and use of personal data in direct marketing (a) The direct marketing industry will be seriously affected by the adoption of an "opt-in" mechanism. (b) An opt-out mechanism should continue to be adopted for direct marketing purpose but more specific requirements should be added to ensure transparency and full disclosure of information to allow consumers to opt out. (c) A "tick-box" should be provided to make it as easy as possible for consumers to opt out and consumers should be given another opportunity to opt out if new use of the personal data is contemplated. (d) According to the findings of the survey conducted by the Association, there is no country where an opt-in mechanism has been adopted exclusively for direct

No.	Deputation [LC Paper No. of submission]	Views and suggestions
		marketing. The opt-in mechanism has only been adopted for e-mail marketing in some overseas countries. Prohibition against transfer of personal data to place outside Hong Kong except in specified circumstances (e) Implementation of section 33 of PDPO is supported which, in its view, will not have adverse impact on the direct marketing industry. However, enforcement of the provision can be an issue. Others (f) The proposal of imposing criminal penalties for certain crimes is supported.
6.	Hong Kong Telemarketer Association [LC Paper No. CB(2)354/10-11(01)]	*Proposal 1: Collection and use of personal data in direct marketing (a) It is unfair to step up regulation on direct marketing activities such as person-to-person telemarketing conducted directly by data users which are generally accepted by the general public. (b) An "opt-out" mechanism should be adopted for direct marketing activities. (c) The direct marketing sector will be seriously affected resulting in abundant job loss if an "opt-in" mechanism is adopted. (d) The proposed requirement of stating the intended direct marketing activities in the personal information collection statement should not be imposed as it is difficult to specify the usage of personal data amid the fast changing business environment.

No.	Deputation [LC Paper No. of submission]	Views and suggestions
		(e) The proposal of raising penalty level for misuse of personal data in direct marketing is too harsh to frontline staff. (f) Different degrees of regulation over different types of personal information can be imposed as follows: - basic information such as name, telephone number and address of data subjects, which can be easily obtained through existing available channels (i.e. name cards, internet, telephone company) should not be subjected to any regulation; - consent of data subjects should be sought for collection and usage of their bank account/credit card/identity card numbers etc; and - transfer of information such as bank account balances, transactions records and credit ratings of data subjects should not be allowed under any circumstances.
7.	Hong Kong Exhibition and Convention Industry Association [LC Paper No. CB(2)317/10-11(03)]	*<u>Proposal 1: Collection and use of personal data in direct marketing</u> (a) An "opt-out" mechanism should be adopted to facilitate operations of exhibitions and trade fairs which target at enterprises on a business to business basis as only basic business contacts with no sensitive personal information will be collected. (b) The exhibition and convention industry will be at stake if an "opt-in" mechanism is adopted as trade partners or professional organizations will be reluctant to share their membership lists to avoid the risk of breaching the law.

No.	Deputation [LC Paper No. of submission]	Views and suggestions
		Prohibition against transfer of personal data to place outside Hong Kong except in specified circumstances (c) Implementation of section 33 of PDPO may affect the operation of the exhibition and convention industry as transfer of data to overseas countries is a frequent and common practice.
8.	Teledirect Hong Kong Ltd. [LC Paper No. CB(2)354/10-11(02)]	*Proposal 1: Collection and use of personal data in direct marketing (a) The proposals of introducing measures and imposing criminal penalties to better regulate the use of personal data is generally supported. (b) An "opt-out" mechanism should be adopted for direct marketing activities and a "tick-box" should be provided in marketing materials to allow consumers to opt out from direct marketing promotion activities.
9.	Hong Kong Call Centre Association ("HKCA") [LC Paper No. CB(2)354/10-11(02)]	
10.	The Hong Kong Federation of Insurers	*Proposal 1: Collection and use of personal data in direct marketing (a) The adoption of an "opt-out" mechanism for collecting personal data is supported. (b) A central Do-not-call register on person-to-person telemarketing should be established. *Proposal 7: Legal assistance to data subjects under section 66 of PDPO (c) PCPD should provide guidance and advice instead of legal assistance to an aggrieved data subject as the legal aid system is well-established in Hong Kong.

No.	Deputation [LC Paper No. of submission]	Views and suggestions
		(d) Mediation services should be provided by PCPD whenever necessary. <u>Others</u> (e) The meaning of some terms in the proposed amendments to PDPO such as "Intentional", "Repeated contravention" and "Indicated disagreement" is too general and should be well defined in legislation. (f) PCPD should step up promotion of the guidelines to raise public awareness about the protection of personal data. (g) The Administration should provide more resources to PCPD to promote proper business conduct and best practice in the protection of personal data instead of merely resorting to legal measures.
11.	Public Services Monitoring Group [LC Paper No. CB(2)353/10-11(01)]	*<u>Proposal 1: Collection and use of personal data in direct marketing</u> (a) An "opt-in" mechanism should be adopted for direct marketing activities except for membership schemes which reward consumers with promotional benefits for collection of their personal data. (b) PCPD should be granted the power to stipulate the scopes of personal data which can be collected from data subjects in specific trades and business sectors such as financial institutions.

No.	Deputation [LC Paper No. of submission]	Views and suggestions
		*<u>Proposal 2: Unauthorized sale of personal data by data user</u> (c) The proposal of stepping up deterrent measures for intrusion of privacy and raising penalty for misuse of personal data is supported. (d) The proposed requirement that the presentation of information in the personal data collection statement should be reasonably readable by general public is supported. *<u>Proposal 5: Regulation of data processors and sub-contracting activities</u> (e) An "opt-in" mechanism should be adopted to regulate transfer of personal data from enterprises to their subsidiary companies and other offshore companies, particularly to offshore call centers. (f) The proposal of requiring a data user to use contractual or other means to ensure the compliance of its data processors and sub-contractors offshore with the requirements under PDPO is supported. #<u>Proposal 39: Granting criminal investigation and prosecution power to PCPD</u> (g) Criminal investigation and prosecution power should be granted to PCPD.

No.	Deputation [LC Paper No. of submission]	Views and suggestions
12.	Mr Roderick WOO Former Privacy Commissioner for Personal Data [LC Paper No. CB(2)353/10-11(02)]	*<u>Proposal 1: Collection and use of personal data in direct marketing</u> (a) The proposal of introducing additional specific requirements to impose stricter regulation on data users in their use (including transfer) of the personal data collected for direct marketing purpose is supported. (b) Inclination to support the continued adoption of an "opt-out" mechanism in direct marketing activities. Data subjects should be given the "opt-out" option to choose any one or more of the direct marketing purposes that he/she disagrees and such "opt-out" option should be separately provided so that individual can clearly indicate the preferences. (c) A central Do-not-call register on person-to-person telemarketing should be established to facilitate individuals expressing their preferences. *<u>Proposal 2: Unauthorized sale of personal data by data user</u> (d) The proposals of imposing additional requirements and introducing criminal offences are supported. *<u>Proposal 6: Personal data security breach notification</u> (e) A mandatory personal data security breach notification system should be put in place in phases. Public sector should be required to give notifications at an initial stage and the requirement should be extended to selected classes of data users in private sector having regard to the degree of sensitivity of personal data and assessment on the impact of leakage.

No.	Deputation [LC Paper No. of submission]	Views and suggestions
		#Proposal 38: Sensitive personal data (f) Sensitive personal data should be subjected to more stringent regulation. (g) A list of sensitive personal data should be compiled in consultation with the public with a view to applying different degrees of regulation according to the categorization of sensitive personal data in future. #Proposal 39: Granting criminal investigation and prosecution power to PCPD (h) Criminal investigation and prosecution power should be granted to PCPD as PCPD is more proficient in interpreting and applying the provisions of PDPO and time to refer cases to the Police can be saved. #Proposal 40: Empowering PCPD to award compensation to aggrieved data subjects (i) PCPD should be empowered to award compensation to aggrieved data subjects. The power to conduct hearing in public (j) PCPD should be empowered under section 43 of PDPO to conduct public hearing for cases of great public concern. Time limit for responding to PCPD's investigation or inspection report (k) The existing requirement under section 46 of PDPO of allowing a data user a period of 28 days to object to the disclosure of any personal data in the

No.	Deputation [LC Paper No. of submission]	Views and suggestions
		inspection/investigation report that are exempted from the provisions of data protection principle 6 should be removed for reports which do not contain personal data.
13.	Professor John Bacon-Shone Former Chairman of the Law Reform Commission [LC Paper No. CB(2)363/10-11(01)]	*<u>Proposal 1: Collection and use of personal data in direct marketing</u> (a) If an "opt-out" mechanism is adopted, it is suggested that data subjects should be offered an opt-out option specific to each purpose of the personal data collected. (b) In addition to the right to be informed of the sources of their personal data, data subjects should have the right to retain control over their personal data such as the right to know about transfer destinations of their personal data, the right to correct or delete their personal data. *<u>Proposal 6: Personal data security breach notification</u> (c) Voluntary notification is inadequate. (d) PCPD should be notified of cases where there is serious potential damage arising from leaked personal data such as disclosure of financial and medical data with personal identifiers so that PCPD will be in the best position to access the risks and decide whether notifications should be issued to the affected data subjects. (e) It should be mandatory for the data users to notify the affected data subjects in cases when there is chance of leakage of personal data and potential damage of data subjects is also expected.

No.	Deputation [LC Paper No. of submission]	Views and suggestions
		#Proposal 38: Sensitive Personal Data (f) Classes of sensitive data should be defined in legislation for additional protection as follows : - authentication/identification data (e.g. biometric features) - reputational data (e.g. HIV status) - group membership that could be discriminated against (e.g. homosexuality/ ethnic origins) - location of people for the protection against spousal abuse or stalking. #Proposal 40: Empowering PCPD to award compensation to aggrieved data subjects (g) The proposal to empower PCPD to award compensation to aggrieve data subjects is the most efficient mechanism to address damages of data subjects. (h) If the proposal to empower the PCPD to award compensation to data subjects is not pursued, the two privacy civil torts (i.e. the tort of intrusion upon another's solitude or seclusion and the tort of unwarranted publicity) proposed by the Law Reform Commission should be enacted to allow data subjects to seek damages for unfair collection and unfair release of personal data.

Appendix V

Relevant documents on the
Review of the Personal Data (Privacy) Ordinance

Committee	Date of meeting	Paper
Legislative Council	2.6.1999	Official Record of Proceedings (Written question No. 18)
	14.3.2001	Official Record of Proceedings Pages 10 - 16 (Oral question)
	2.5.2001	Official Record of Proceedings Pages 50 - 64 (Written question)
	27.11.2002	Official Record of Proceedings Pages 53 - 55 (Written question)
Panel on Information Technology and Broadcasting ("ITB Panel")	1.11.2005 (Item I)	Agenda Minutes LS21/05-06 CB(1)1233/06-07(01)
Home Affairs Panel ("HA Panel")	8.11.2005	Minutes
ITB Panel	17.3.2006 (Item IV)	Agenda Minutes
Legislative Council	26.4.2006	Official Record of Proceedings Pages 34 - 41 (Oral question)
	3.5.2006	Official Record of Proceedings Pages 86 - 88 (Written question)
ITB Panel	11.12.2006 (Item VI)	Agenda Minutes
HA Panel	9.2.2007 (Item IV)	Agenda Minutes Report on Civil Liability for Invasion of Privacy published by the Law Reform Commission in December 2004

Committee	Date of meeting	Paper
Legislative Council	7.3.2007	Official Record of Proceedings Pages 75 - 77 (Written question)
	2.5.2007	Official Record of Proceedings Pages 80 - 82 (Written question)
	4.7.2007	Official Record of Proceedings Pages 88 - 90 (Written question)
ITB Panel	9.7.2007 (Item V)	Agenda Minutes
Legislative Council	20.2.2008	Official Record of Proceedings Pages 82 - 84 (Written question)
	21.5.2008	Official Record of Proceedings Pages 44 - 56 (Oral question) Pages 89 - 91 (Written question)
	28.5.2008	Official Record of Proceedings Pages 7 - 16 (Oral question)
ITB Panel	30.5.2008	Agenda Minutes CB(1)1875/07-08(01)
HA Panel	4.7.2008 (Item I)	Agenda Minutes
Constitutional Affairs Panel ("CA Panel")	23.10.2008 (Item I)	Agenda Minutes
Legislative Council	26.11.2008	Official Record of Proceedings Pages 74 - 76 (Written question)
CA Panel	11.9.2009 (Item I)	Agenda Minutes
	18.10.2010 (Item III)	Agenda

Committee	Date of meeting	Paper
Legislative Council	20.10.2010	Official Record of Proceedings Pages 145 - 242 (Motion)
CA Panel	15.11.2010 (Item IV)	Agenda
	20.11.2010 (Item I)	Agenda
	20.12.2010 (Item III)	Agenda
Legislative Council	12.1.2011	Official Record of Proceedings Pages 126 - 209 (Motion)
	6.4.2011	Official Record of Proceedings (Written question)

Council Business Division 2
Legislative Council Secretariat
14 April 2011