立法會
Legislative Council

LC Paper No. CB(2)237/11-12(04)

Ref : CB2/BC/8/10

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

Background brief prepared by the Legislative Council Secretariat

Purpose

This paper provides background information on the review of the Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO") and summarizes the relevant issues raised by members of the Panel on Constitutional Affairs ("the CA Panel").

Background

2. 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.

3. At present, a contravention of a DPP is not an offence. It is only upon the breach of an enforcement notice ("EN") issued after the completion of an investigation that the relevant data user 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.

4. 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 the Privacy Commissioner for Personal Data ("PCPD") to assist data subjects in claiming damages.

5. 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.

6. 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. 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, 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.

Major issues raised by the CA Panel

Relevant meetings

7. At its special meeting on 11 September 2009, the CA Panel discussed the Consultation Document. At its meetings on 18 October, 15 November and 20 December 2010, the CA Panel discussed the Report on Public Consultation on Review of PDPO ("the Consultation Report") which was issued in October 2010 for further public consultation. The Administration set out the proposals to be taken forward and those which would not be pursued in the Consultation Report. The Panel also received views from the deputations on the Consultation Report at its meeting on 20 November 2010. A summary setting out the views and suggestions of the deputations is in **Appendix I**.

8. Following the publication of the Report on Further Public Discussions on Review of PDPO, the Administration further briefed the CA Panel at its meeting

on 18 April 2011 on the result of the further public consultation on review of PDPO conducted from October to December 2010 and the legislative proposals drawn up in the light of the views received.

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

Enforcement powers of PCPD

10. Some members expressed concern that the Administration did not propose to grant criminal investigation and prosecution powers 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. They further queried whether the Police had sufficient resources and expertise to conduct criminal investigation into cases involving contravention of PDPO referred by the Office of PCPD.

11. 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 domain as the existing practice of vesting in separate authorities the powers of criminal investigation, prosecution and judging on criminal cases had been functioning well.

12. It was the Administration's view that the existing arrangements, under which the powers to conduct criminal investigation, prosecute and give ruling on criminal cases were separately vested with the Police, the Department of Justice ("DoJ") and the Judiciary in order to ensure a fair trial and judicial independence, had been functioning well and should not be changed lightly. The Administration also advised that to afford better protection of personal data privacy, the Administration had proposed to introduce in PDPO additional specific requirements on data users for the collection and use of personal data for direct marketing, to make unauthorized sale of personal data an offence, and to increase the penalty level for repeated non-compliance with EN etc. On granting additional sanctioning powers to PCPD, the Administration had proposed to empower PCPD to provide legal assistance to an aggrieved data subject to institute legal proceedings to seek compensation under section 66 of PDPO. PCPD should continue to exercise his investigation power available under the existing framework of PDPO and put more emphasis on education and complaint handling work as an advocate for privacy protection.

13. 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.

14. PCPD, however, considered that the recent cases of contravention of PDPO and unauthorized sale of personal data had reflected the inadequacy of the enforcement powers of PCPD. The proposal of granting PCPD criminal investigation and prosecution powers could meet the public expectation for enhancing deterrence 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 for 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.

Unauthorized collection, use and sale of personal data

15. 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 did not need to bear any legal consequences provided that they had subsequently complied with the EN.

16. 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 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.

17. The Administration further explained that it was proposed to adopt a two-step approach 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.

18. 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.

19. 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.

<u>"Opt-in" and "opt-out" mechanism for collection and use of personal data</u>

20. Some members expressed strong support for the Administration's proposal for adopting an "opt-out" mechanism for collection and use of personal data on the grounds that it could facilitate business developments 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.

21. Some other members, however, expressed strong dissatisfaction at the Administration's proposal. They took the view that adopting an "opt-out" mechanism did not afford adequate safeguards to the personal data as explicit consent of consumers was not required. It was suggested that different mechanisms for collection and use of personal data could be adopted having regard to the purpose of collection. For instance, an opt-in mechanism could be adopted for sale of personal data whereas an opt-out mechanism could be adopted for transfer of personal data which did not involve monetary or in kind gain.

22. The Administration advised that it intended to adopt an "opt-out" mechanism for collection and use of personal data in direct marketing and sale of personal data having regard to the experiences of overseas countries. The Administration emphasized that an "opt-out" mechanism could strike a balance between safeguarding the personal data privacy of the public and facilitating business operations.

23. PCPD 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. Nevertheless, 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 setting up 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 unsolicited promotion calls using personal data.

24. Some members were also of the view that a data user should notify the data subject of the source of his personal data for direct marketing purpose and the data subject would be given the right to request any data user to notify both the transferee who held the source of his personal data and the classes of persons to whom his personal data had been transferred for direct marketing to cease using and transferring the data. The Administration, however, advised that as the personal data of the public were probably collected from diverse channels by a data user, it would be difficult for a data user to trace the sources and notify all the data users concerned to cease using the data. Under the Administration's proposal, a data subject could request a data user to notify the classes of persons to whom his personal data had been transferred for direct marketing to cease using the data.

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

25. Members in general expressed support for the proposal for empowering PCPD to provide legal assistance to an aggrieved data subject to institute legal proceedings to seek compensation under section 66 of PDPO to enhance the sanctioning powers of PCPD. The Administration advised that the proposal would be implemented following the existing model of the Equal Opportunities Commission to provide legal assistance to complainants.

Data security and protection of privacy on the Internet

26. 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.

27. 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.

28. 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.

29. 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

30. 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.

31. The Administration explained 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.

Relevant papers

32. A list of the relevant papers available on the LegCo website is in **Appendix II.**

Council Business Division 2
Legislative Council Secretariat
7 November 2011

LC Paper No. CB(2)582/10-11(06)

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	*Proposal 1: Collection and use of personal data in direct marketing (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. *Proposal 6: Personal data security breach notification (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)]	*Proposal 1: Collection and use of personal data in direct marketing (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. *Proposal 6: Personal data security breach notification (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. #Proposal 38: Sensitive personal data (d) The Administration should introduce a categorization system for sensitive personal data with a view to affording better protection of such data. #Proposal 39: Granting criminal investigation and prosecution Power to PCPD (e) Criminal investigation and prosecution power should be granted to PCPD. #Proposal 43: Parents' right to access personal data of minors (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 II

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

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 Minutes

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 Pages 13 - 15 (Written question)
CA Panel	18.4.2011 (Item IV)	Agenda

Council Business Division 2
Legislative Council Secretariat
7 November 2011