立法會
Legislative Council

LC Paper No. CB(2)37/10-11(03)

Ref : CB2/PL/CA

Panel on Constitutional Affairs

Updated background brief prepared by the Legislative Council Secretariat for the meeting on 18 October 2010

Review of the Personal Data (Privacy) Ordinance (Cap. 486)

Purpose

This paper provides background information on the review of the Personal Data (Privacy) Ordinance (Cap. 486) ("PD(P)O") and summarises the relevant issues raised by various panels since the First Legislative Council ("LegCo").

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 PD(P)O on 3 August 1995. PD(P)O was brought into force on 20 December 1996.

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

The Ordinance

4. PD(P)O 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 PD(P)O 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 enforcement notice 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. PD(P)O 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. PD(P)O 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 the requirements of the Ordinance 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 PD(P)O

8. 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. The Panel on Home Affairs ("the HA Panel") discussed the progress of the review with the Constitutional and Mainland Affairs Bureau ("CMAB") and the Privacy Commissioner at its meeting on 4 July 2008. While the amendment proposals prepared by PCPD required further deliberation within the Administration, the Administration had briefed the Panel on its initial thinking in respect of the following proposals put forward by PCPD -

(a) the handling of sensitive personal data including racial or ethnic origin, political affiliation, religious beliefs, membership of trade unions, physical or mental health, biometric data and sexual life should be prohibited unless specified circumstances were met in order to provide a higher degree of protection towards such data and contravention of the prohibition would be made an offence;

(b) the Privacy Commissioner should be vested with direct prosecution power;

(c) particular acts or practices such as knowingly or recklessly obtaining or disclosing personal data held or leaked by a data user, or the subsequent sale of the personal data so obtained should be singled out as criminal offence in order to achieve deterrent effect; and

(d) the penalty level for certain acts of contravention such as a second or subsequent breach of an enforcement notice should be raised.

9. According to the Administration, a major objective of the comprehensive review of PD(P)O 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. The Administration informed the HA Panel that it was studying the various amendment proposals and, after assessment of their implications, would consult LegCo and the public. The Administration aimed at coming up with concrete proposals to amend PD(P)O for consultation with the Fourth LegCo as early as possible.

10. Members of the HA Panel considered that the review progress of PD(P)O should be expedited in order to tackle problems arising from advancement in technology and to afford better protection to personal data. The comments made by individual members of the HA Panel on the amendment proposals put forward by PCPD included –

(a) the protection afforded by PD(P)O was inadequate and the Privacy Commissioner's lack of direct prosecution power as well as the need to make contravention of a DPP an offence should be reviewed;

(b) the proposal of providing a higher degree of protection towards sensitive personal data should be supported;

(c) while the proposal of conferring the Privacy Commissioner with direct prosecution power should be supported, the fundamental principle that the control of criminal prosecutions must be vested in the Department of Justice ("DoJ") should be upheld and delegation of this prerogative should not be made on a permanent basis;

(d) the proposal of introducing a mandatory privacy breach notification requirement in case of breaches where there was a high risk of significant harm and of expanding the definition of "personal data" to deem Internet Protocol ("IP") addresses as "personal data" should be supported; and

(e) the proposal of amending the Ordinance to deal with the use of personal data when there was overriding public interest, particularly in emergency situation should be supported.

11. With effect from the 2008-2009 legislative session, the policy area of personal data protection has been placed under the purview of the Panel on Constitutional Affairs ("the CA Panel"). The Administration informed the CA Panel in October 2008 that as the review of PD(P)O covered fundamental issues which affected individuals' rights and civil liberties, the Administration was working with PCPD to assess the feasibility and impact of amendment proposals prior to public consultation.

12. On 28 August 2009, the Administration, with the support of PCPD, issued the Consultation Document on Review of the PD(P)O ("the Consultation Document") to invite public views on the proposals to amend the Ordinance. The consultation period ended on 30 November 2009. According to the Administration, conduct of the review is guided by the following factors -

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

(b) balance is 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 is a need to avoid putting onerous burden on business operations and individual data users;

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

(f) PD(P)O should remain flexible and relevant in spite of technological change;

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

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

13. At the special meeting of the CA Panel held on 11 September 2009, the Administration and the then Privacy Commissioner briefed members on the major proposals in the Consultation Document and the major areas of difference in views between the Administration and PCPD. The major proposals and those proposals which the Administration had considered but was inclined not to pursue as extracted from the Consultation Document are in **Appendix I** and **Appendix II** respectively.

Issues relevant to the review raised by LegCo panels

14. The main issues raised by members of the CA Panel and other Panels concerning review on PD(P)O are summarized below.

Scope of "personal data" under PD(P)O

15. In October 2005, it was widely reported by local newspapers that Yahoo! Holdings (Hong Kong) Limited ("YHHK") had disclosed user information corresponding to an IP address of a journalist who was an email user of Yahoo! China residing in the People's Republic of China ("PRC"), leading to his arrest and conviction of the crime of illegally providing state secrets to foreign entities outside PRC ("the Yahoo case"). At its meeting held on 1 November 2005, the Panel on Information Technology and Broadcasting ("the ITB Panel") discussed issues related to the protection of personal information of email account subscribers.

16. In accordance with the definition of "personal data" under section 2(1) of PD(P)O, the data must satisfy the requirements of identifiability and retrievability in order to constitute "personal data". "Data" is defined to mean any representation of information (including an expression of opinion) in any document, and includes a personal identifier. Under PD(P)O, a personal identifier means an identifier that is assigned to an individual by a data user for the purpose of the operations of the user and that uniquely identifies that individual in relation to the data user, but does not include an individual's name used to identify that individual. Pursuant to section 38(b) of PD(P)O, if the Privacy Commissioner has reasonable grounds to believe that an act or practice has been done or engaged in, or is being done or engaged in, by a data user, and such an act or practice relates to personal data and may be a contravention of a requirement under the Ordinance, he may carry out an investigation in relation to the data user, even though no complaint is received.

17. It was the PCPD's preliminary view at that time that the email user information allegedly furnished by the e-mail service provider in the Yahoo case only identified a business entity from which it might not be practicable to ascertain the identity of a living individual directly or indirectly. Hence the information might not amount to "personal data" as defined under PD(P)O and PCPD had not initiated an investigation under section 38 of PD(P)O. PCPD explained that in determining whether the data in question was "personal data" under PD(P)O, one of the criteria was that the identity of a living individual could be directly or indirectly ascertained from the data.

18. Some members of the ITB Panel did not subscribe to the preliminary views taken by PCPD on the interpretation of "personal data". They were worried that protection for privacy might have been undermined if PCPD had all along adopted such a narrow interpretation of the term "personal data". They considered that the Privacy Commissioner should re-examine what information would amount to "personal data" as defined under PD(P)O in order that the purpose of protecting personal data would not be defeated. If necessary, consideration should be given to review PD(P)O.

19. Members may wish to note that in its report on the Yahoo case published on 14 March 2007 ("the PCPD report") (LC Paper No. CB(1)1233/06-07(01)), PCPD remained of the view that an IP address per se does not meet the definition of "personal data" under PD(P)O (paragraph 8.11 of the report). Members may also wish to note that in its paper entitled "Scope of 'personal data' under the Personal Data (Privacy) Ordinance (Cap. 486) and related issues" prepared for the ITB Panel (LC Paper No. LS21/05-06), the Legal Service Division of the LegCo Secretariat raised the following policy issues -

(a) whether it was necessary to ask the Administration to review whether PD(P)O offered adequate protection to personal data collected on the Internet having regard to the development of technology; and

(b) whether specific legislation or additional privacy principles were necessary to address the issues of privacy and data protection on the Internet with reference to the approaches adopted by some overseas jurisdictions. For example, Germany had included in its Teleservices Data Protection Act 1997 provisions dealing with issues associated specifically with the use of Internet. In the Directive on Privacy and Electronic Communications adopted by the European Union in 2002, there were provisions dealing with the confidentiality of communications made over a public electronic communications network, the use of cookies and the inclusion of personal data in public directories.

20. When the Yahoo case was raised again at the CA Panel meeting on 11 September 2010, Mr Albert HO expressed disappointment that the Administrative Appeals Board, which investigated the complaint lodged against the email service provider for infringing the provisions of PD(P)O by disclosure of an email subscriber's personal data, concluded that the IP address and the log-in information of the subscriber's e-mail account did not constitute personal data within the definition of PD(P)O. Mr HO considered that applying such a restrictive interpretation of the term "personal data" defined in PD(P)O and the transfer of personal data from Hong Kong to another jurisdiction which did not have comparable personal data protection system had tarnished the reputation of Hong Kong. He expressed concern that the power of IP providers to disclose personal data of their subscribers and to pass intelligence to another authority would be unchecked, and this would infringe the personal data privacy of data subjects.

21. The then Privacy Commissioner maintained the view that the IP address per se might not amount to "personal data" as defined under PD(P)O and hence PCPD could not conduct an investigation on the case. In light of the Yahoo case, PCPD had suggested to the Administration to review whether IP address should be regarded as "personal data" within the definition of PD(P)O and to consider whether the collection and use of personal data outside Hong Kong by a data user in Hong Kong should be regulated by PD(P)O; as well as to consult the public on the definition of "crime" under the exemption provision of PD(P)O (i.e. section 58).

22. The Administration reiterated that it had reservations about deeming IP address per se as "personal data" as it would place an unreasonable burden on and pose serious compliance problems to various industry players in the information technology industry. There was a need to strike a balance between protection of personal data privacy and normal business operation.

Application of PD(P)O

23. According to its letter dated 28 October 2005 addressed to the Chairman of the ITB Panel, YHHK advised that while both Yahoo! Hong Kong and Yahoo! China websites were previously owned by the company, the later was now owned and controlled by another corporation[1]. Yahoo! Hong Kong adhered to all applicable local laws and regulations in Hong Kong while Yahoo! China adhered to all applicable local laws and regulation in PRC. PCPD advised the ITB Panel at its meeting on 1 November 2005 that generally speaking, if the collection and use of personal data took place outside Hong Kong, the handling of such information would not be covered by PD(P)O which only had jurisdiction in Hong Kong. However, the definition of "data user" under PD(P)O meant a person who, either alone or jointly or in common with other persons, controlled the collection, holding, processing or use of the data. The key question was whether YHHK in actual operation was able to control, in or from Hong Kong, either alone or jointly with Yahoo! China, the collection and use of the personal data in question.

24. Some members of the ITB Panel queried how a data user in Hong Kong such as YHHK could comply with the laws and regulations of the Mainland as well as those of Hong Kong at the material time when there were conflicting requirements between the two systems, and how far YHHK was bound by the requirements under PD(P)O for the disclosure of information of its email account subscribers to the Mainland authorities.

25. Members may wish to note that the then Privacy Commissioner in the PCPD report found it an opportune time to review the sufficiency of the provisions of PD(P)O in respect of the scope of application of the Ordinance to the following situations -

(a) where none of the act of collection, holding, processing and use of the personal data took place in Hong Kong; and

(b) where disclosure of personal data was made pursuant to a lawful requirement imposed by a foreign authority for the purpose of investigation of a foreign crime.

Note[1] In its information subsequently provided to PCPD, YHHK advised, among others, that the data which the case concerned was collected by Yahoo! China in PRC, which was owned by YHHK at the material time and the data in question was disclosed by Yahoo! China in PRC to the PRC authorities in accordance with PRC law and YHHK had no control over the collection and/or disclosure of Yahoo! China's users data.

26. The Privacy Commissioner also recommended the Administration to consider legislative amendments -

(a) in order to quell any uncertainty hinging around the meaning of "control" of personal data and the extraterritorial application of PD(P)O;

(b) to give clear definitions of the words "crime" and "offenders" in section 58 of the Ordinance so that it would facilitate the data user to assess and determine whether the exemption provision under section 58 of the Ordinance could be properly invoked in any particular circumstances of the case[2].

Unauthorized obtaining, disclosure and sale of personal data

27. At the CA Panel meeting on 11 September 2010, 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.

28. The Administration advised that Proposal No. 8 in the Consultation Document suggested 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. Several issues needed to be further deliberated if the proposed offence was to be implemented, for example, whether a person with a reasonable defence should or should not be held liable.

29. The then Privacy Commissioner, however, expressed concern that Proposal No. 8 of criminalizing the act of disclosing data for profits or malicious purposes could not plug the loophole of the existing legal framework. Under the existing legislation, exemption from PD(P)O was given to personal data held by an individual for domestic or recreational purposes. In a recent case, a Taxation Officer of the Inland Revenue Department who had recorded the personal particulars of 13 400 taxpayers for his personal future use was acquitted from the charge of misconduct in public office because the prosecution could not prove that his collection of taxpayers' personal data was intended for profits or malicious use.

Note[2] DPP 3 provides that unless the data subject gives consent, otherwise personal data should be used for the purposes for which they were collected or a directly related purpose. Pursuant to section 58 of PD(P)O, personal data are exempt from the application of this Principle where the data is disclosed for the purposes of the prevention or detection of crime, or the apprehension, prosecution or detention of offenders, etc.

Implementation of section 33 of PD(P)O

30. When the Panel on Financial Affairs was briefed at its meeting on 24 September 2002 on the proposal on the sharing of positive credit data in the consultation document issued by PCPD, concern was expressed about the possible abuse of positive credit data when such data were transferred to jurisdiction outside Hong Kong. The then Privacy Commissioner explained that section 33 of PD(P)O stipulated that data users in Hong Kong were prohibited from transferring data to another territory where comparable privacy protection was lacking. Section 33, however, was the only provision which had not commenced operation. It was understandable that to put this provision into force would have significant and far-reaching bearing on cross-boundary business operations. As an interim measure, in the event that personal data were to be transferred and put to use outside Hong Kong, some degree of privacy protection could be attained by way of a contractual undertaking made between the data user in Hong Kong and the institution which handled the data outside Hong Kong.

31. When the HA Panel received a briefing from the then Privacy Commissioner on his work plan at its meeting on 8 November 2005, PCPD advised that after an investigation into cross-boundary dataflow practices in the banking sector in Hong Kong in late 2004, the Office had provided a report with a range of policy options to the Administration. According to PCPD, those policy options ranged from maintaining the status quo to the full implementation of section 33, but the Administration had not responded on these options. As there were significant consequences for Hong Kong and data users arising from any decision to bring section 33 into operation, careful scrutiny and a public consultation exercise would be warranted.

32. At the CA Panel meeting on 11 September 2009, Mr IP Kwok-him expressed concern that the Consultation Document was silent on the implementation of section 33 which was the only provision which had not commenced operation. The Administration responded that PCPD had taken some time to consider how to implement section 33. Under the provision, one of the permitted circumstances for transfer of personal data outside Hong Kong was that the place to receive the personal data had in place an acceptable data protection regime. Commencement of section 33 necessitated PCPD to specify places with law substantially similar to, or served the same purposes as PD(P)O. The then Privacy Commissioner, however, advised that PCPD was ready to implement section 33, pending the Administration's decision.

Statutory powers of the Privacy Commissioner and enforcement powers of PCPD

33. Arising from a series of incidents relating to leakages of personal data through the Internet and losses of portable electronic storage devices containing such data which involved government bureaux/departments and public as well as private bodies, the ITB Panel discussed issues relating to information security at a number of meetings held on 17 March and 11 December 2006, 9 July 2007 and 30 May 2008 respectively. According to the information provided by the Administration for the

period from May 2005 to May 2008, the numbers of citizens affected by these incidents were 1 884 for cases occurring in government bureaux/departments and 44 339 for cases occurring in public bodies.

34. The then Privacy Commissioner advised the ITB Panel that breaches of DPPs of PD(P)O and improper use of data for personal gain were not criminal offences. It was only upon the issuance of an enforcement notice and the failure to comply with the terms of the enforcement notice that an offence would be committed. Section 64(10) of PD(P)O expressly excluded contravention of DPPs from the scope of offence provided in the said section. Moreover, if a data user failed to comply with the enforcement notice issued to him/her under section 50 of PD(P)O, the Privacy Commissioner would need to forward a detailed report to the Police for investigation. If the case was substantiated, DoJ would be asked to consider taking prosecution action under section 64(7). There might be duplication of investigation effort resulting in unnecessary delay in the prosecution of substantiated cases. The then Privacy Commissioner considered that as the Ordinance had been in force for nearly a decade, it was time to review whether more serious punishment should be imposed on infringement of the Ordinance including making it a criminal offence for any person to obtain, disclose or sell personal data held by a data user, without the data subject's consent, and whether the Privacy Commissioner should be conferred with criminal investigation and prosecution powers.

35. Some members of the ITB Panel expressed support for providing the Privacy Commissioner with criminal investigation and prosecution powers. They stressed that it was timely to review PD(P)O to assess its efficacy or otherwise in the face of technological advancement.

36. At the CA Panel meeting on 11 September 2009, Mr Ronny TONG enquired why the Administration did not support the proposal of granting criminal investigation and prosecution power to PCPD (Proposal No. 4 of the Consultation Document). Dr Margaret NG, however, did not support Proposal No. 4 and considered that prosecution power should be vested in an independent body in accordance with the existing constitutional framework. The proposal to confer criminal investigation and prosecution power on PCPD would give rise to conflict of interests as PCPD was the enforcer of PD(P)O.

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

(a) under the Basic Law, the control of criminal prosecutions was vested in DoJ. Although it would not be inconsistent with the Basic Law to confer prosecution power on PCPD if the relevant legislation expressly stated that the prosecutions to be brought there under 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 attached great importance to these principles and had reservations about conferring the power of criminal investigation, prosecution and imposing penalty on one single authority;

(c) the appropriate body to determine compensation under PD(P)O 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. LRC opined 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. LRC recommended that PCPD's role should be limited to determining whether there had been a breach of DPPs. It would be for the court to determine the appropriate amount of compensation payable. The Administration shared the same view but would invite views on whether it was appropriate to introduce an additional redress avenue by empowering PCPD to award compensation to aggrieved data subjects;

(d) it was not common for non-judicial bodies to have the statutory power to impose monetary penalties. In addition, whether an act constituted a serious contravention of a DPP was a matter of subjective judgment. The Administration would invite views on whether it was appropriate to empower PCPD to impose monetary penalty for serious contravention of DPPs;

(e) if PCPD was empowered to offer legal assistance to an aggrieved data subject who suffered damage to seek redress under PD(P)O, the aggrieved party would be in a better position to assess the chance of success of his civil claim and would not be inhibited from filing a lawsuit due to cost considerations. The proposal, if pursued, could achieve greater deterrent effect on acts or practices which intruded into personal data privacy, and enhance the overall effectiveness of sanctions provided for under PD(P)O; and

(f) as regards creating new criminal offences, the Administration was aware of the need to give specific and clear legislative intent in its proposals and to set a higher threshold for criminalizing certain acts. On measures to step up enforcement, Proposal No. 5 proposed to provide legal assistance to an aggrieved data subject so that he or she would have the means to file a lawsuit when the case warranted it, and Proposal No. 40 proposed to extend the time limit for laying information for prosecution of an offence under PD(P)O.

38. PCPD, however, took the view that the Privacy Commissioner, who possessed the expertise and first hand information on a case, could act expeditiously to deal with the suspected offence if he was granted the criminal investigation and prosecution power. 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. The proposal to confer prosecution power on PCPD was formulated taking into account the views of some members of the ITB Panel expressed earlier, and PCPD was open-minded about the proposal.

Parents' right to access personal data of minors and transfer of personal data of minors relevant to parental care and guardianship

39. At the CA Panel meeting on 11 September 2009, Dr Priscilla LEUNG considered that Proposal Nos. 14 and 27 in the Consultation Document which sought to restrict parents' right to access personal data of minors had projected a negative image of parents. She pointed out that there were concerns about parents being restricted from accessing personal data of minors who were very young and the right of a social worker to decline parents' request for access to personal data of the child.

40. The Administration considered that it was important 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. The then Privacy Commissioner explained that by virtue of section 18(1) of PD(P)O, a parent had the right to make a request on behalf of his/her child to access the child's personal data. Proposal No. 14 which was put forward by PCPD sought to address exceptional cases where the child had expressed to the data user his/her disagreement to the disclosure of his/her personal data to his/her parents. The proposal was formulated having regard to the concerns raised by some social workers who had been faced with the dilemma of whether or not to accede to parents' data access request to disclose the child's personal information confided in them. The proposal sought to provide a ground of refusal that a social worker might exercise if disclosure of the child's personal data to the parent would not be in the best interests of the child.

Reporting and notification arrangements

41. Some members of the ITB Panel expressed concern about the lack of a standard practice among government bureaux/departments to alert the affected data subjects or report the incidents to the Hong Kong Police Force and/or PCPD, given the possible serious consequences that could be caused to these data subjects. They also pointed out that as there were no statutory requirements for data users to report leakage of personal data to PCPD, the Office could only come to know about leakage through media enquiries and press reports. The Administration advised that whether the reporting and notification practice should be made mandatory would be examined in the review of PD(P)O.

Civil claim for compensation under PD(P)O

42. When consulting the HA Panel on the major recommendations made by LRC on the protection of privacy at its meeting on 9 February 2007, the Administration advised that according to the Report on Civil Liability for Invasion of Privacy, provisions of PD(P)O were concerned only with privacy in relation to personal data, not privacy rights in general. Examples of privacy rights were privacy of the person, territorial privacy and communications and surveillance privacy. As the Privacy Commissioner did not have the power and resources to provide assistance to aggrieved individuals who wished to make a civil claim under section 66 of PD(P)O, victims who had suffered damage by reason of a contravention of a DPP had to bear all the legal costs unless they were entitled to legal aid. This was contrary to the position of the Equal Opportunities Commission under the Sex Discrimination Ordinance (Cap. 480) ("SDO") and the Disability Discrimination Ordinance (Cap. 487) ("DDO"). LRC therefore recommended in the Report that PD(P)O be amended to enable the Privacy Commissioner to provide legal assistance to data subjects who intended to institute proceedings under section 66 of PD(P)O, along the lines of section 85 of SDO and section 81 of DDO.

43. According to the Administration, legislative amendments would be introduced on this recommendation which had the support of both the Administration and the Privacy Commissioner. It was envisaged that the legislative amendments, if enacted, could strengthen the deterrent effect on likely offenders of personal data privacy law, thereby affording better protection of the public against intrusion of privacy.

44. In response to the enquiry raised during the CA Panel meeting on 11 September 2009 about the civil liabilities imposed on persons leaking personal data, the Administration advised that under the existing law, a data subject who suffered damage by reason of a contravention of a requirement under PD(P)O 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 and to enhance the overall effectiveness of sanctions provided for under PD(P)O, Proposal No. 5 in the Consultation Document further suggested conferring on PCPD the power to provide legal assistance to aggrieved data subjects. With the provision of legal assistance, an aggrieved party would then not be inhibited from filing a lawsuit due to cost considerations.

Recent development

45. In July 2010, it was widely reported by the media that Octopus Rewards Limited, a company wholly owned by Octopus Holdings Limited had passed Octopus cardholders' personal data collected under the Octopus Rewards Programme to third parties for direct marketing purpose. The incident had aroused wide public concern regarding the handling of personal data by Octopus Rewards Limited and the need to enhance the relevant legislation for the protection of personal data. Mr WONG Kwok-hing has given notice to move a motion on "Improving personal data privacy protection" for debate at the Council meeting on 20 October 2010.

46. The Administration is scheduled to brief the CA Panel on the outcome of the review of PDPO and the legislative proposals at its meeting on 18 October 2010.

Relevant questions raised at Council meetings

47. A list of relevant questions raised by Members at Council meetings since the First LegCo is in **Appendix III**.

Relevant papers

48. A list of relevant papers available on the LegCo website (http://www.legco.gov.hk) is in **Appendix IV.**

Council Business Division 2
Legislative Council Secretariat
15 October 2010

Sensitive Personal Data

Proposal No. 1: Sensitive Personal Data

8. At present, the PDPO does not differentiate personal data that are "sensitive" from those that are not. More stringent regulation of sensitive personal data is in line with international practices. However, there is no universally agreed set of sensitive personal data and perception of sensitive personal data is culture-bound. Given the challenges posed by the development of biometric technology on an individual's privacy, as a start we may consider classifying biometric data (such as iris characteristics, hand contour reading and fingerprints) as sensitive personal data.

9. To provide a higher degree of protection to sensitive personal data, we have set out in the consultation paper a possible regulatory model to limit the handling of sensitive personal data by data users to specified circumstances in order to narrow down the scope of collection and use of such data.

Data Security

Proposal No. 2: Regulation of Data Processors and Sub-contracting Activities

10. The rising trend of data users sub-contracting and entrusting data processing work to third parties has increased the risk to which personal data may be exposed. At present, the PDPO does not regulate processors which process personal data for data users. To strengthen security measures governing personal data entrusted to data processors, we have set out possible regulatory options.

11. Under such options, a data user who transfers personal data to a data processor for holding, processing or use, would be required to use contractual or other means to ensure that his data processor and any sub-contractors will take all practicable steps to ensure the security and safekeeping of the personal data, and to ensure that the data are not misused and are deleted when no longer required for processing.

12. As part of the options, we can consider directly regulating data processors by imposing obligations on them. They would be required to exercise the same level of due diligence as the data user with regard to security, retention and use of the personal data thus entrusted.

Recognising that compliance with certain requirements may pose problems for some data processors due to the operational constraints unique to specific industry sectors, we have also included the option of subjecting different categories of data processors to different obligations.

Proposal No. 3: Personal Data Security Breach Notification

13. Following the spate of personal data leakage incidents, questions have been raised on whether a personal data security breach notification ("privacy breach notification") system should be instituted to require data users to notify the PCPD and affected individuals when a breach of data security leads to the leakage or loss of personal data so as to mitigate the potential damage to affected individuals. A mandatory notification requirement could impose undue burden on business operations. Bearing in mind that a number of overseas jurisdictions adopt voluntary guidelines on privacy breach notifications, we consider it more prudent to start with a voluntary breach notification system so that we can assess the impact of breach notifications more precisely, and fine-tune the notification requirements to make them reasonable and practicable, without causing onerous burden on the community. For this purpose, the PCPD can issue guidelines on voluntary privacy breach notifications.

Enforcement Powers of the PCPD

Proposal No. 4: Granting Criminal Investigation and Prosecution Power to the PCPD

14. At present criminal investigations are conducted by the Police and prosecutions by the Department of Justice. We have considered if these powers should be conferred on the PCPD. Since some offences proposed in this review are not technical in nature and involve a fine and imprisonment, there could be concern if such powers are delegated to the PCPD. Moreover the existing arrangements have worked well. We do not see a strong case to give the PCPD the power to investigate into and prosecute criminal offence cases.

Proposal No. 5: Legal Assistance to Data Subjects under Section 66

15. Under Section 66 of the Ordinance, a data subject who suffers damage by reason of a contravention of a requirement under the PDPO by a data user in relation to his personal data is entitled to compensation from the data user. The PDPO does not empower the PCPD to provide

assistance to aggrieved data subjects in respect of legal proceedings. To achieve greater deterrent effect on acts or practices which intrude into personal data privacy and enhance the overall effectiveness of sanctions provided for under the PDPO, views are invited on whether the PCPD should be conferred the power to provide legal assistance to an aggrieved data subject.

Proposal No. 6: Award Compensation to Aggrieved Data Subjects

16. We have considered whether the PCPD should be empowered to determine the amount of compensation to a data subject who suffers damage by reason of a contravention of a requirement by a data user, as an alternative to the existing redress avenue to seek compensation through the court as provided for under Section 66 of the PDPO. The appropriate body to determine compensation under the PDPO was thoroughly discussed in the Law Reform Commission ("LRC") Report on Reform of the Law Relating to the Protection of Personal Data issued in August 1994. The LRC opined 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. The LRC recommended that the PCPD's role should be limited to determining whether there has been a breach of the Data Protection Principles ("DPPs"). It would be for a court to determine the appropriate amount of compensation payable. Views are invited on whether it is appropriate to introduce an additional redress avenue by empowering the PCPD to award compensation to aggrieved data subjects.

Offences and Sanctions

Proposal No. 7: Making Contravention of a Data Protection Principle an Offence

17. The PCPD is empowered to remedy contravention of a DPP by issuing an enforcement notice to direct the data user to take remedial steps. Contravention of the enforcement notice is an offence.

18. One option is to consider making contravention of a DPP an offence. Bearing in mind that DPPs are couched in generic terms and can be subject to a wide range of interpretations, to make contravention of a DPP a criminal offence would have significant impact on civil liberties if an inadvertent act or omission could attract criminal liability. Moreover, this would be moving away from the original intent of adopting the DPPs in the PDPO. Views are invited on whether we

should make contravention of a DPP an offence.

Proposal No. 8: Unauthorized Obtaining, Disclosure and Sale of Personal Data

19. Incidents of blatant dissemination of leaked personal data on the Internet have aroused widespread concern in the community regarding the possible misuse of leaked personal data, such as fraud or identity theft. Unauthorised use of personal data may also intrude into personal data privacy and may cause damage to data subjects. To curb irresponsible dissemination of leaked personal data, we may consider making it an offence if a person obtains personal data without the consent of the data user and discloses the personal data so obtained for profits or malicious purposes.

Proposal No. 9: Repeated Contravention of a DPP on Same Facts

20. Under the PDPO, if a data user who, having complied with the directions in an enforcement notice to the satisfaction of the PCPD, subsequently does the same act or engages in the same practice, the PCPD would issue another enforcement notice. Since the enactment of the PDPO, PCPD has not come across any such case of circumvention. To forestall possible circumvention of the regulatory regime, one option is to consider making it an offence if a data user repeats such contravening act. However, this would be moving away from the original intent of adopting the DPPs in the PDPO. Views are invited on whether this is appropriate.

Proposal No. 10: Imposing Monetary Penalty on Serious Contravention of DPPs

21. We have considered the option of empowering the PCPD to require data users to pay monetary penalty for serious contravention of DPPs. It is not common for non-judicial bodies to have the statutory power to impose monetary penalties. Under the PDPO, the DPPs are couched in generic terms and can be subject to wide interpretations. Although we may require the PCPD to issue guidance on the circumstances he considers appropriate to issue a monetary penalty notice, whether an act constitutes a serious contravention of a DPP is a matter of subjective judgment. Views are invited on whether it is appropriate to empower the PCPD to impose monetary penalty on serious contravention of DPPs.

Proposal No. 11: Repeated Non-compliance with Enforcement Notice

22. The PDPO does not provide for heavier sanction for data users who repeatedly contravene an enforcement notice. Since the enactment of the PDPO, there has not been a problem with repeated offenders. We have considered the option to subject a repeated offender to heavier penalty to achieve greater deterrent effect. Views are invited on whether there is a need to impose a heavier penalty for such repeated offenders.

Proposal No. 12: Raising Penalty for Misuse of Personal Data in Direct Marketing

23. Direct marketing calls are often a cause of complaint and nuisance to the data subjects. The PCPD is of the view that the existing level of a fine at Level 3 (up to $10,000) may not be sufficient to act as an effective deterrent to contain the problem and recommends the penalty level be raised. To curb misuse of personal data in direct marketing activities, we may consider raising the penalty level for misuse of personal data in direct marketing. Public views are invited on the appropriate level of penalty.

Proposals not to be Pursued

1. We have considered a number of proposals relating to scope of regulation of the PDPO, and exemptions from the provisions of the PDPO. After deliberating on the implications of the proposals, we are not inclined to pursue them. They are set out in paragraphs 2 to 29 below.

(A) Scope of Regulation under the PDPO

A.1 Revamping Regulatory Regime of Direct Marketing

2. Section 34 of the PDPO regulates the use of personal data in carrying out direct marketing activities by data users. It requires a data user who has obtained personal data and use such data for direct marketing purposes to inform the data subject of his opt-out right. The data user shall not use such personal data for carrying out direct marketing activities, if the data subject has requested the data user to cease to so use his personal data. A data user who, without reasonable excuse, contravenes this requirement commits an offence and is liable on conviction to a fine at Level 3 (up to $10,000).

3. To address the proliferation of uncontrolled direct marketing activities, we have examined the possibility of revamping the regulatory regime for direct marketing activities under the PDPO. The options include :

   (a) to introduce a new requirement that when personal data are used for direct marketing for the first time, the data user has to obtain the explicit consent of the data subject for the use of the latter's personal data (i.e. "opt-in" choice); and

   (b) to set up a territorial wide central Do-not-call register against direct marketing activities.

4. The objective of the PDPO is to protect personal data privacy of individuals. Section 34 of the PDPO already regulates the use of personal data in direct marketing. To guard against misuse of personal data in direct marketing, we have put forth the proposal to raise the penalty level of contravention of the requirements under Section 34 (please refer to Proposal No. 12).

5. Direct marketing activities in the form of electronic communications (other than person-to-person telemarketing calls) are regulated by the UEMO. The Administration is monitoring the situation of using person-to-person calls for telemarketing purpose and will consider the possibility of regulating such activities under the UEMO if the problem grows in future.

6. In the circumstances, we do not consider it appropriate to make further amendments to Section 34 of the PDPO.

A.2 Internet Protocol Address as Personal Data

7. In March 2006, the PCPD received a complaint alleging the disclosure of an email subscriber's personal data by email service provider had infringed the provisions of the PDPO. One of the crucial issues to be considered was whether an Internet Protocol address ("IP address") alone would be regarded as personal data within the definition of the PDPO. Separately, there were suggestions that the Government should review the PDPO and adopt measures to prohibit the disclosure of IP addresses to third parties by email service providers without the authorization of the subscribers.

8. An IP address is a unique number to enable electronic devices to identify and communicate with each other on a computer network. When an electronic device communicates with others through the Internet, an IP address has to be assigned to it for identification purpose. In his investigation report dated March 2007 on the above-mentioned complaint case, the PCPD took the view that an IP address per se does not meet the definition of "personal data", because IP address is about an inanimate device, not an individual. It alone can neither reveal the exact location of the electronic device concerned nor the identity of the user.

9. There is a lack of judicial authority on whether IP address constitutes personal data. There is also no universally or internationally recognized definition on personal data. For reference, the Data Protection Working Party of the European Union ("EU") considered that in most cases IP addresses relate to identifiable persons. In this regard, personal data is defined in Article 2(a) of the EU Directive as any information relating to an identified or identifiable natural person, and an identifiable

person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

10. There is a need to strike a balance between protection of personal data privacy and normal business operation. Deeming IP address per se as personal data would pose unreasonable burden on and serious compliance problems for various industry players in the information technology industry. For instance, it is not practicable for the industry to comply with DPP 4 (security of personal data principle) because an IP address is a piece of addressing information that flows through different parties in the Internet world outside the control of a single ISP or network operator. Moreover, an IP address, if combined with other identifying particulars of an individual, will be afforded protection under the PDPO. Deeming an IP address as personal data also begs the question as to why cookies, email address, mobile phone number, vehicle registration mark, Autotoll tag number, Octopus card number, etc, cannot likewise be regarded as personal data under the PDPO since they are also capable of "indirectly" identifying a particular individual through tracing. In the circumstances, we do not consider it appropriate to deem IP address per se as personal data under the PDPO.

A.3 Territorial Scope of the PDPO

11. At present, the PDPO applies where a data user controls the processing of data in or from Hong Kong even if the whole data processing cycle occurs outside Hong Kong. The PCPD proposes that the PDPO should not apply where none of the acts of the data processing cycle takes place in Hong Kong, mainly because of enforcement difficulties. In their view, the mere presence, without more, of a person in Hong Kong who has the ability to control his business abroad, which collects, holds, processes or uses personal data, is generally not sufficient to attract or to enable the PCPD to assume jurisdiction under the Ordinance.

12. The territorial scope of the data protection law for Hong Kong was thoroughly discussed by the LRC in 1994, on the basis of which the Administration decided on the span of control under the PDPO. This was based on the model of the United Kingdom.

The LRC considered it important that data protection law in Hong Kong should apply to a data user within the jurisdiction, even where the data have been transferred to or are being processed in another jurisdiction. This approach also applies to the provisions relating to transborder data flow.

13. The proposal in paragraph 11 above might create a loophole in our control regime in that a company in Hong Kong can bypass the PDPO by arranging offshore collection of personal data through an agent and outsource the holding, processing and use of personal data to offshore agent(s). This may risk Hong Kong being turned into a data haven free of effective controls on personal data, which would not be in the interest of promoting the free flow of data to Hong Kong. We are not inclined to pursue this proposal.

(B) Exemptions

B.1 Public Interest Determination

14. At present, specific exemptions from subject access (DPP 6 and Section 18(1)(b)) and DPP 3 are provided for under Part VIII of the PDPO on grounds of specified public interests, including security, defence and international relations in respect of Hong Kong (Section 57), law enforcement and regulation (Section 58) and health (Section 59). The PDPO, however, does not contain a general provision that makes the protection of public interest itself a justification for exemption.

15. To provide for regulatory flexibility when public interest outweighs the degree of intrusion into personal data privacy, we may consider adding a new provision to empower the Privacy Commissioner to make a public interest determination (including a temporary public interest determination for applications which require urgent decision), with conditions, if any, imposed on a case-by-case basis upon application by the relevant data user.

16. The existing exemptions provisions under the PDPO strikes a balance between privacy rights and public interest in specific circumstances. The proposed public interest determination provision will be operated on an ad hoc and a case by case basis. Such a mechanism if instituted will undermine the certainty of personal data privacy protection afforded to data subjects. As

such, we do not consider it appropriate to pursue such a proposed provision. If there are justifications to grant exemption on specific grounds, it is more appropriate to address them by way of specific public interest exemptions.

B.2 Public Domain Exemption

17. The PCPD proposes to provide for a new exemption from DPP 3 (use of personal data principle) for personal data available in the public domain. In making this proposal, the PCPD acknowledges that there are problems of using publicly available information for secondary purposes. These include the use of property owners' records from the Land Registry to provide a search of an individual's property ownership, the use of personal data contained in public register for direct marketing activities, and the improper use of personal data available on the Internet arising from data leakage incidents. On the other hand, there may be legitimate purposes to serve in checking an individual's financial status, such as property ownership, before deciding whether to institute legal proceedings or pursue enforcement actions against that individual.

18. The LRC had carefully deliberated on whether data protection laws should completely exempt public registers. The LRC expressed concerns that an exemption would sanction data collected for specific purposes being used for another purpose not originally envisaged by the person furnishing the data. They concluded that "there should be an exemption from the application of the Use Limitation Principle (i.e. DPP 3) for data which are required by or under any enactment to be made available to the public" but "should the data be applied for another purpose, the data protection law would apply at that point."

19. There is no public domain exemption in personal data protection laws of the UK, New Zealand and Australia. In our view, putting personal data in the public domain does not make the data available for use for any purpose. If the test for exemption is simply whether the data are in the public domain, it would provide data users with the opportunity to subvert the law by publicizing the data. The proposal could result in abuse in the use of information available in the public domain, such as improper use of personal data available on the Internet arising

from data leakage incidents. We do not see a case to take this proposal forward.

(C) Powers of the PCPD

C.1 Power to Search and Seize Evidence

20. The PCPD is empowered under the PDPO to be furnished with any information, document or thing from any person, enter premises, summon witnesses, and conduct hearing. The Privacy Commissioner, however, has no power to search and seize evidence. The PCPD proposes that the Commissioner be equipped with the power to search and seize evidence in order to gather evidence for prosecution proceedings.

21. The existing provisions of the PDPO are to address the concern voiced during the legislative process that this newly established investigative body should not be vested with full powers of search and seizure. Similar concern was shared by the LRC. While the LRC believed that powers to enter premises and obtain evidence are necessary to enable the Commissioner to carry out his functions, the data user's consent should first be sought but, if that is not forthcoming, the court should be empowered to make an appropriate order for entry and seizure.

22. The additional powers proposed are to facilitate the PCPD to carry out criminal investigations. Since we do not see a strong case to grant the PCPD criminal investigation and direct prosecution power (see Proposal 4 in Chapter 5), there is no need to provide these additional powers to the Privacy Commissioner. We also consider the existing investigative power of the PCPD adequate. In the circumstances, we are not inclined to take forward the proposal.

C.2 Power to Call upon Public Officers for Assistance

23. In the exercise of the PCPD's power of investigation and inspection, the Privacy Commissioner may need to enter premises. Where resistance or obstruction is encountered, the PCPD would need to seek assistance from the police. Expert advice and assistance are also required in investigation. These include information technology and computer forensics, identification of suspects by use of digital images, and reconstruction of criminal

activities requiring software analysis, reverse engineering decryption and presentation of digital data. At present, the PCPD is not empowered under the PDPO to call upon public officers to assist him in his discharge of investigation and inspections. He can only rely on the goodwill of public officers for assistance. The PCPD proposes to provide the Privacy Commissioner with an express power to call upon public officers to assist him in performing the regulatory functions under the PDPO. The PCPD envisages that an express provision would be necessary when he is conferred with the power to investigate offence and institute prosecution.

24. Public officers have all along been providing assistance to the PCPD in the discharge of his regulatory functions in the absence of a specific provision to such effect in the PDPO. We do not see a need for specific provisions in the PDPO if the Privacy Commissioner simply requests assistance of officers of government departments. In this regard, it is an offence under Section 64(9) of the PDPO for a person who, without lawful excuse, obstructs, hinders or resists the Privacy Commissioner or any other person in the performance of his functions or the exercise of his powers under Part VII (inspections, complaints and investigations). In the circumstances, an express provision as proposed by the PCPD would not be necessary.

C.3 Power to Conduct Hearing in Public

25. Section 43(2) of the PDPO provides that any hearing for the purpose of an investigation shall be carried out in public unless the Privacy Commissioner considers otherwise or the complainant requests that the hearing be held in private. The PCPD opines that the provision will hinder the Commissioner from holding the hearing in public, particularly when issues of public interest and importance are involved and when members of the public have a genuine right to know and to be informed. We have considered whether the Privacy Commissioner should be conferred the power to decide whether a hearing should be held in public having regard to all the circumstances of the case including any request made by a complainant.

26. The right to demand a private hearing by the data subject is a conscious recommendation made by the LRC on grounds that the prospect of a public hearing could act as a real disincentive to the

lodging of a complaint. As regards overseas practice, Australia requires conferences in relation to a complaint to be conducted in private, and New Zealand has similar requirement for the conduct of investigations.

27. The LRC considerations for granting the data subject the right to demand a private hearing are still valid today. We do not see a need to change the system. In this regard, Section 48(2) of the PDPO empowers the Privacy Commissioner to publish a report on the result of the investigation as well as the recommendations thereof, if he is in the opinion that it is in the public interest to do so. The right of the public to know and be informed can, to a certain extent, be taken care of in that context.

C.4 Time Limit for Responding to PCPD's Investigation/Inspection Report

28. A data user is currently allowed under Section 46(4)(b) to advise the Privacy Commissioner within 28 days whether he objects to the disclosure in the report on inspection or investigation prepared by the PCPD any personal data that are exempt from the provisions of DPP 6 by virtue of Part VIII (exemptions) of the PDPO before its publication. The PCPD proposes to shorten the period from 28 days to 14 days on the ground that the present response period of 28 days hinders timely reporting of matters of public interest.

29. We envisage that data users in some cases may need to circulate the report for comments and seek legal advice before they can provide an official response to the PCPD. Such a course of action takes time. A response period of 14 days is unreasonably tight. In our view, shortening of the response period by 14 days will not significantly improve the timeliness of publication of an inspection or investigation report. We do not consider it appropriate to take forward the proposal.

Appendix III

Questions relevant to the review of the Personal Data (Privacy) Ordinance (Cap. 486) raised at Council meetings since the first Legislative Council

Meeting Date	Question
2.6.99	Hon SIN Chung-kai raised a written question on whether e-mail addresses were classified as personal data under the Personal Data (Privacy) Ordinance and their disclosure to third parties.
14.3.01	Hon Audrey EU raised an oral question on whether government departments using the Owners' Properties Information Check Service to conduct searches of memorial had contravened provisions of the Personal Data (Privacy) Ordinance.
2.5.01	Hon Audrey EU raised a written question on the disclosure of personal data of members of the public by government departments in the context of the relevant exemption provisions in the Personal Data (Privacy) Ordinance.
27.11.02	Hon Timothy FOK raised a written question on the review of the Personal Data (Privacy) Ordinance to enhance the protection of the privacy of public figures.
26.4.06	Hon James TO raised an oral question on the review of the Personal Data (Privacy) Ordinance.
3.5.06	Hon SIN Chung-kai raised a written question on whether Internet Protocol addresses were regarded as personal data under the Personal Data (Privacy) Ordinance and their disclosure to third parties.
7.3.07	Hon TSANG Yok-sing raised a written question on section 33 of the Personal Data (Privacy) Ordinance on "Prohibition against transfer of personal data to place outside Hong Kong except in specified circumstances", which was not yet in operation.
2.5.07	Hon Emily LAU raised a written question on whether the Personal Data (Privacy) Ordinance would be reviewed to enhance the protection of personal data.
4.7.07	Hon Albert HO raised a written question on the review of the Personal Data (Privacy) Ordinance and issues concerning personal data faced by Hong Kong companies doing business in the Mainland.
20.2.08	Hon Albert HO raised a written question on the progress of the review of the Personal Data (Privacy) Ordinance.

Meeting Date	Question
21.5.08	Hon Emily LAU raised a written question on the review of the Personal Data (Privacy) Ordinance.
	Hon Audrey EU raised an oral question on protection of personal data.
28.5.08	Hon TSANG Yok-sing raised an oral question on protection of personal data by government departments and public organizations.
26.11.08	Hon CHEUNG Hok-ming raised a written question on whether the unauthorized disclosure of personal data by credit card-issuing bodies to debt collection agencies had contravened provisions of the Personal Data (Privacy) Ordinance.

Council Business Division 2
Legislative Council Secretariat
15 October 2010

Appendix IV

Relevant documents on the Review of the Personal Data (Privacy) Ordinance (Cap. 486)

Meeting	**Meeting date**	**Paper**
Panel on Information Technology and Broadcasting ("ITB Panel")	1 November 2005	Submission from the Office of the Privacy Commissioner for Personal Data on Issues related to the Protection of Personal Information of E-mail Account Subscribers [LC Paper No. CB(1)160/05-06(01)] Administration's paper on "Licensing Framework for Internet Service Providers and Protection of Personal Data" [LC Paper No. CB(1)173/05-06(01)] Speaking note of the Privacy Commissioner for Personal Data [LC Paper No. CB(1)211/05-06(01)] Minutes of meeting [LC Paper No. CB(1)412/05-06] Letter dated 28 October 2005 from Yahoo! Holdings (Hong Kong) Limited to the Chairman of ITB Panel [LC Paper No. CB(1)186/05-06(03)] Paper prepared by the Legal Service Division on scope of "Personal Data" under the Personal Data (Privacy) Ordinance (Cap. 486) and related issues [LC Paper No. LS21/05-06] Report of the Office of the Privacy Commissioner for Personal Data published under Section 48(2) of the Personal Data (Privacy) Ordinance (Cap. 486) [LC Paper No. CB(1)1233/06-07(01)]
Home Affairs Panel ("HA Panel")	8 November 2005	Minutes of meeting [LC Paper No. CB(2)577/05-06]
ITB Panel	17 March 2006	Submission from the Office of the Privacy Commissioner for Personal Data on Information Security [LC Paper No. CB(1)1093/05-06(02)]

Meeting	**Meeting date**	**Paper**
		Administration's paper on "Information Security" [LC Paper No. CB(1)1097/05-06(01)] Minutes of meeting [LC Paper No. CB(1)1382/05-06]
	11 December 2006	Administration's paper on "Information Security" [LC Paper No. CB(1)435/06-07(05)] Background brief on Information Security [LC Paper No. CB(1)435/06-07(06)] Minutes of meeting [LC Paper No. CB(1)669/06-07]
HA Panel	9 February 2007	Report on Civil Liability for Invasion of Privacy published by Law Reform Commission in December 2004 Administration's paper on "Protection of Privacy" [LC Paper No. CB(2)1014/06-07(01)] Background brief on Reports published by the Law Reform Commission on privacy [LC Paper No. CB(2)1014/06-07(02)] Minutes of meeting [LC Paper No. CB(2)1501/06-07]
ITB Panel	9 July 2007	Administration's paper on "Information Security" [LC Paper No. CB(1)2034/06-07(04)] Updated background brief on Information Security [LC Paper No. CB(1)2063/06-07(01)] Minutes of meeting [LC Paper No. CB(1)2396/06-07]

Meeting	**Meeting date**	**Paper**
	30 May 2008	Administration's paper on "Information Security" [LC Paper No. CB(1)1679/07-08(01)] Administration's paper on "Data leakage incidents involving various bureaux/ departments for the last 3 years up to 22 May 2008 [LC Paper No. CB(1)1875/07-08(01)] Minutes of meeting [LC Paper No. CB(1)2311/07-08]
HA Panel	4 July 2008	Administration's paper on "Review of the Personal Data (Privacy) Ordinance" [LC Paper No. CB(2)2488/07-08(01)] Administration's paper on "Protection of Personal Data Privacy" [LC Paper No. CB(2)2454/07-08(01)] Speaking note of the Privacy Commissioner for Personal Data [LC Paper No. CB(2)2528/07-08(01)] Information note on "Implementation problems of the Personal Data (Privacy) Ordinance" prepared by Research and Library Services Division of the Legislative Council Secretariat [LC Paper No. IN21/07-08] Minutes of meeting [LC Paper No. CB(2)2850/07-08]
Constitutional Affairs Panel ("CA Panel")	23 October 2008	Administration's paper on "2008-09 Policy Agenda" [LC Paper No. CB(2)72/08-09(01)]
	11 September 2009	Consultation Document on Review of the Personal Data (Privacy) Ordinance Administration's paper on "Consultation Document on Review of the Personal Data (Privacy) Ordinance" [LC Paper No. CB(2)2410/08-09(01)]

Meeting	**Meeting date**	**Paper**
		Background brief on "Review of the Personal Data (Privacy) Ordinance (Cap. 486)" prepared by the Legislative Council Secretariat [LC Paper No. CB(2)2445/08-09(01)] Office of the Privacy Commissioner for Personal Data's paper on "Consultation Document on Review of the Personal Data (Privacy) Ordinance" [LC Paper No. CB(2)2473/08-09(01)] PCPD's information paper on "Review of the Personal Data (Privacy) Ordinance" [LC Paper No. CB(2)2473/08-09(02)] Minutes of meeting [LC Paper No. CB(2)684/09-10]

Council Business Division 2
Legislative Council Secretariat
15 October 2010