LC Paper No

(PCPD's Paper for LegCo meeting on 20.11.2010)

LEGISLATIVE COUNCIL

Panel on Constitutional Affairs

Special meeting on Saturday, 20 November 2010, at 9 a.m.
in the Chamber of the Legislative Council Building

Agenda Item I – Report on Public Consultation on Review of the Personal Data (Privacy) Ordinance

Background

1. In August 2009, the Constitutional and Mainland Affairs Bureau (CMAB) issued the "Consultation Document on Review of the Personal Data (Privacy) Ordinance" ("Consultation Document"). The public consultation ended on 30 November 2009. For the consultation exercise, the Office of the Privacy Commissioner for Personal Data ("PCPD") has prepared and submitted to CMAB in November 2009 a paper entitled "PCPD's Submissions to Consultation Document on Review of the Personal Data (Privacy) Ordinance" setting out PCPD's point of views on various proposals. A copy of the paper is enclosed.

2. On 18 October 2010, the Administration released the "Report on Public Consultation on Review of the Personal Data (Privacy) Ordinance" ("Consultation Report") setting out the views received and the Administration's proposed way forward on various proposals. In light of the widespread concerns in the community about the transfer of customer's personal data by some organizations for direct marketing purposes, the Administration has also formulated some new proposals to enhance the protection of personal data privacy. Views are invited on the specific arrangements and details of the 37 proposals to be taken forward until 31 December 2010.

3. The PCPD welcomes the Administration's determination in affording a higher level of personal data protection in Hong Kong in pursuing 37 proposals,

the majority of which was made by the PCPD to the CMAB in December 2007. However, the PCPD is concerned that some proposals to step up protection of personal data privacy are not to be pursued or taken forward in the Consultation Report. The major ones are as follows:-

Areas	Proposals
Revamping Regulatory Regime of Direct Marketing	**Proposal 1 –** Collection and Use of Personal Data in Direct Marketing **–** (b) Requiring data user to obtain explicit and voluntary consent of data subject to use personal data for direct marketing purpose ("Opt-in" regime); (c) Setting up a territory - wide "Do-not-call" register; (d) Conferring on individuals a right to be informed of the source of personal data by direct marketers.
Sanctioning Power	**Proposal 39** – Granting Criminal Investigation and Prosecution Power to the PCPD (Considered together with the powers to Search and Seize Evidence and to Call upon Public Officers for Assistance (Annex 5 of the Consultation Report))
	Proposal 40 – Empowering the PCPD to Award Compensation to Aggrieved Data Subjects
	Proposal 42 – Empowering the PCPD to Impose Monetary Penalty on Serious Contravention of Data Protection Principles
Tackling privacy concerns caused by data processors and outsourcing activities	**Proposal 5 –** Direct Regulation of Data Processors and Sub-contracting Activities

Harnessing Impact on Personal Data Privacy Caused by Technological Advancement	**Proposal 38 –** More stringent regulation on Sensitive Personal Data

Major Areas of Difference in Views between the Administration and the PCPD

Revamping Regulatory Regime of Direct Marketing

Proposal 1 *– Collection and Use of Personal Data in Direct Marketing*

(a) Requiring data user to obtain explicit and voluntary consent of data subject to use personal data for direct marketing purpose ("Opt-in" regime)

4. The opposing reason given in the Consultation Report is that the "opt-in" proposal will add burden to the operations of enterprises carrying out direct marketing activities, and the setting up of a territory-wide Do-not-call register on person-to-person telemarketing goes beyond the protection of personal data privacy.

5. However, there are clear voices expressed in the consultation exercise and the recent Octopus incident that more stringent regulation on the collection and use of personal data for direct marketing activities should be imposed. The PCPD takes the view that introducing an "opt-in" regime is consistent with the overwhelming public expectation for greater self-determination.

6. While the Administration has made a new proposal to strengthen the regulation on the collection and use of personal data in direct marketing activities, it remains an "opt-out" approach in that the customers are invited, at the time when they provide their personal data to organizations, to "opt-out" from direct marketing promotion activities. The beauty of the PCPD's approach, on the other hand, is that the data subject's preference is made known directly and without doubt.

(b) Setting up a territory-wide "Do-not-call" register;

7. The setting up of a territory-wide "Do-not-call" register to deal with person-to-person telemarketing calls involving personal data will further curb the problem of inconvenience caused by these calls. The PCPD keeps an open mind on whether this should be an independent register created and run by the PCPD or that this should be incorporated in the Office of the Telecommunications Authority's Do-not-call register, or that of any other public agencies.

(c) Conferring on individuals a right to be informed of the source of personal data by direct marketers

8. The PCPD had suggested to the Administration earlier to impose an obligation on a direct marketer to disclose the source of the personal data upon the data subject's request.[1] The Australian Law Reform Commission made a similar recommendation in its Report 108 – For Your Information: Australian Privacy Law and Practice. The Australian Government has accepted the recommendation that individuals should have the right to be so informed by the organization if they have not had a customer relationship with the organization.[2] As a result of the Administration's new proposals on direct marketing and Proposal 2 (Unauthorized Sale of Personal Data by Data User), it is pertinent that a direct marketer will be required to disclose the source of their personal data when so requested by a data subject. This will facilitate the data subject to trace the culpable ones on suspected contraventions of these new offences by the relevant data users.

9. The PCPD is aware of the concerns of direct marketers including that on employment opportunities. While an 'opt-in' regime may cause the number of callers employed to detune, the quality of the calls, both in terms of their acceptability to the recipients and the success in closing a sale, is likely to improve. That direct marketing activities will become more cost-effective and

[1] See page 155, Issue 2, Annex to the PCPD's Information Paper on Review of the Personal Data (Privacy) Ordinance and p.60-61 of PCPD's Submissions to Consultation Document on Review of the Personal Data (Privacy) Ordinance (available at http://www.pcpd.org.hk/english/review_ordinance/files/Odnreview_Information_Paper_e.pdf and http://www.pcpd.org.hk/english/review_ordinance/files/PCPD_submission_ReviewPDPO_e.pdf).

[2] Recommendation 26-6 Australian Government First Stage Response to ALRC Privacy Report (available at http://www.dpmc.gov.au/privacy/alrc_docs/stage1_aus_govt_response.pdf)

less annoying is a benefit of PCPD's proposal not to be overlooked.

Sanctioning Power

10. The recent Octopus incident has seen the community up in arms demanding punishment for violation of the Personal Data (Privacy) Ordinance ("PDPO"), reflecting clearly the gap between public expectations and the current powers of the PCPD. In short, there is an inadequacy of enforcement power of the PCPD if public expectations are to be met. Although the Administration finally decided to take forward the PCPD's proposal to relax the restrictions for the PCPD to issue enforcement notice under section 50 of the PDPO (Proposal 8 – Circumstances to Issue Enforcement Notice), that alone is insufficient to step up the current regime in sanctioning data user in serious breaches of data protection principles.

Proposal 39 *– Granting Criminal Investigation and Prosecution Power to the PCPD (considered together with Powers to Search and Seize Evidence and to Call upon Public Officers for Assistance)*

11. The Administration proposed to maintain status quo. Their main reason is that PCPD's proposal may result in a loss of checks and balances and it would be more appropriate for such power to investigate in and prosecute criminal offence be vested with the Police and the Department of Justice respectively.

12. Our view, however, is that the granting of prosecution power to the PCPD will not usurp the Secretary of Justice's power or discretion to prosecute. PCPD's proposal entails only the PCPD carrying out the prosecution work. The discretion whether or not to prosecute always is and shall remain reserved for the Secretary for Justice. Under PCPD's proposal, any prosecution to be initiated by the PCPD shall only be carried out with the consent of the Secretary for Justice. The power and function of prosecution, if vested with the PCPD, entail the due presentation of facts by the PCPD to the Court. It does not place the PCPD in a position to decide or judge the culpability of any data user. That power, as always, stays with the Judiciary.

13. It should be noted that the PCPD is an independent privacy enforcement authority. It is empowered under the PDPO to investigate infringement of personal data privacy by both the public and the private sectors.

Granting criminal investigation and prosecution powers to the PCPD will help avoid criticism of favouritism where the Police or other government departments are involved in the case as data user. Indeed, some complainants prefer the cases to be handled by the PCPD rather than the Police. In PCPD's experience, when asked to give consent for referral of complaint to the Police for criminal investigation, some complainants would refuse immediately.

14. Another opposing reason given by the Administration is the low number of referrals and successful convictions in the past years which does not justify granting the power to the PCPD. It should be noted that whether or not to prosecute, or whether a prosecution results in successful conviction is not in the hands of the PCPD once a case is referred out. The fact is that cases of contravention of the PDPO are generally not considered a priority in the array of offences within the purview of the Police both in terms of seriousness and urgency.

15. If the number of cases is one consideration in this regard, it should be noted that with the Administration's agreement to take forward the proposals on 6 new offences and the extension of time to lay prosecution and relaxation of the PCPD's discretion to issue enforcement notice, there is a strong likelihood that the prosecution figures will increase substantially in the near future. Listed below is the 6 new offences to be created :-

Proposal 1	–	Collection and Use of Personal Data in Direct Marketing
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
Proposal 18	–	Repeated Contravention of a Data Protection Principle on Same Facts
Proposal 19	–	Repeated Non-compliance with Enforcement Notice
Proposal 27	–	the Offence on Misuse or Excessive Retention of Personal Data in Business Mergers or Acquisition

16. The PCPD believes that it would be in the best interest of the community for enhancement of personal data privacy protection to confer criminal investigation and prosecution powers on the PCPD. While the community may not have been ready to support this proposal last year, the situation may be different now in consequence of the Octopus case which may

only be the tip of the iceberg. The PCPD further considers that the following proposals to strengthen the sanctioning powers of the PCPD should be adopted to enhance deterrent effect.

Proposals 40 and 42 *– Empowering the PCPD to Award Compensation to Aggrieved Data Subjects and to Impose Monetary Penalty on Serious Contravention of Data Protection Principles*

17. The enforcement action to be taken against contravention of the Data Protection Principles ("DPP") in Schedule 1 of the PDPO are limited to serving on the relevant data user an enforcement notice pursuant to section 50(1) of the PDPO directing it to take steps to remedy the contravention. It is only where the data user refuses or fails to comply with the enforcement notice that the data user may then be prosecuted. Proposals 40 and 42, if adopted, will address the public concerns about the sanctioning powers which aim at assisting aggrieved data subjects and penalizing data users for blatant disregard of personal data privacy rights.

18. The major opposing view cited in the Consultation Report is that in the common law system, it is not appropriate to vest in a single authority a combination of enforcement and punitive functions. The PCPD would like to point out that Proposal 40 is modeled on section 52 of the *Australian Privacy Act* and Proposal 42 is modeled on section 55 of the *UK Data Protection Act*. Both Australia and United Kingdom apply the common law system.

19. Proposal 40 (Power to Award Compensation to Aggrieved Data Subjects) will directly address the concern of providing remedy to the aggrieved data subjects without them having to go through prolonged and tedious legal process. The *Australian Privacy Act* provides that if conciliation to resolve a complaint fails, the Australian Privacy Commissioner may, (a) make a declaration directing the respondent to take steps remedying the contravention; and (b) award damages to the complainant. The PCPD may carry out settlement by conciliation and adopt similar approach before making adjudication on the compensation. This way of handling is also consistent with the current judicial approach (post Civil Justice Reform) of adopting mediation between prospective litigants as a default arrangement.

20. It is mentioned in the Consultation Report that aggrieved data subjects would be given sufficient assistance to claim compensation under section 66 of the PDPO by virtue of Proposal 7 (Legal Assistance to Data Subjects under

section 66). However, it is to be noted that Proposal 7 arrangements can only be selectively applied and cannot replace Proposal 40. According to the model of the Equal Opportunities Commission ("EOC") quoted in the Consultation Report, the relevant legislation empowers the EOC to accede to a request for legal assistance under certain conditions only, for instance, where the case raises a question of principle. Hence, an aggrieved data subject will not be assisted if any one of the conditions is not fulfilled. If the aggrieved data subject initiates civil action by himself, what he has to face is usually an organizational data user who has ample resources to contest the civil action. Therefore, the PCPD takes the view that both Proposals 7 and 40 should be taken on board in order to provide sufficient and efficient assistance to the aggrieved data subjects. These two proposals will generate direct and effective deterrent effect on data users against infringement of the PDPO. The PCPD further proposed that an additional power be conferred on the PCPD to carry out mediation of a complaint including settlement by a monetary sum. At present, there is no express provision under the PDPO for the PCPD to carry out mediation of a complaint.

21. In circumstances involving serious and blatant disregard of the personal data privacy rights, the issuance of an enforcement notice directing data user to take remedial steps is considered insufficient. Proposal 42 (Empowering the PCPD to impose Monetary Penalty on Serious Contravention of Data Protection Principles) will equip the PCPD with the power to impose monetary penalty on the data user to achieve the necessary deterrent effect. By reference to the United Kingdom model, the PCPD may serve on a data user a monetary penalty notice where the Commissioner is satisfied that (a) there has been a serious contravention of the data protection principles; (b) the contravention is of a kind likely to cause substantial damage or distress; and (c) the data controller knows or ought to have known a risk of contravention of a kind likely to cause substantial damage or distress but he failed to take reasonable steps to prevent the contravention. The amount of penalty to be determined must not exceed the maximum amount as prescribed. For reference, under the current UK legislation regime, the maximum monetary penalty that the UK Information Commissioner may impose is £500,000.

22. With this power, data users will face significant monetary punishment in serious contraventions of the data protection principles. Examples of cases that the proposed sanction may be imposed are:-

(a) The Octopus incident where personal data of more than 2 million

members were transferred, without the members' voluntary and express consent, to a third party for direct marketing activities for monetary gains;

(b) The Hospital Authority's data loss incident where medical data of patients held in USB flash drives were lost on various occasions;

(c) The IPCC incident where personal data relating to complaints against the Police were leaked out on the Internet.

Tackling privacy concerns caused by data processors and outsourcing activities

Proposal 5 – *Regulation of Data Processors and Sub-contracting Activities*

23. It is the original proposal of the PCPD to bring data processors into the regulatory regime under the PDPO because the current definition of "data user" expressly excludes them by virtue of section 2(12). The PCPD proposed a two-limb regulatory model:-

(a) that data processors should receive **direct regulation** under the PDPO; and

(b) that data user should be required to use **contractual or other means to secure its data processor's compliance** with the relevant obligations under the PDPO.

24. The proposal of **direct regulation** by imposing separate obligations on data processors to comply with DPP 2(2), 3 and 4 is to require them to:-

(a) ensure the personal data will be used only for the purpose for which such data were so entrusted or for directly related purpose;

(b) take all reasonably practicable steps to ensure the security and safeguarding of the personal data under its custody; and

(c) take reasonably practicable steps to erase personal data no longer required for fulfillment of the purpose for which the personal data were so entrusted.

25. The PCPD is concerned that the proposal for data processors to be put under **direct regulation** of the PDPO is not accepted. In particular, the PCPD does not consider it sufficient protection for data subjects by simply relying on data users to regulate their sub-contractors. As was observed in cases in which, for instance, bank client records, which were supposed to have been properly disposed of ended up as wrapping papers used by florists in markets, it is clear that unless data processors are brought under the direct oversight of the PCPD, data subjects will remain vulnerable relying on only contractual and self regulation.

26. The regulatory regime of direct regulation on data processors has been promulgated in overseas data privacy protection laws for many years. For instance, the United Kingdom followed the *European Union Directive 95/46/EC* and the *UK Data Protection Act 1998* specifically provides for the definition of *"data processor"* which essentially means any person who processes the data on behalf of the data controller. Insofar as personal data are entrusted to the processor for processing, it shall assume the role of data controller. The United Kingdom data protection principles impose duty on data controller to implement appropriate technical and organizational measures including (i) the choosing of a data processor providing sufficient guarantees in respect of technical and organizational measures governing the processing of the data; and (ii) the taking of reasonable steps to ensure compliance with those measures by the data processor. Also, Information Privacy Principle 4 of the *Australia Privacy Act* states that if it is necessary for the records containing personal information to be given to a person in connection with the provision of service to the record keeper, it should do *"everything that is reasonable within its power to prevent unauthorized use or disclosure of information contained in the records"*.

27. With regard to the concern expressed in the Consultation Report that data processors do not have any knowledge of the nature or the use of the data and the procedures involved in data processing are complicated, it is to be noted that the risk of any data privacy breach on the part of the Internet Service Providers and web-based service providers is not merely hypothetical or remote. Web-based service providers, such as *Google* and *Yahoo*, handle vast amount of data in their services rendered to customers everyday. Besides, the proposal only requires the ISPs to ascertain the purpose for which they collected the data from the users of their Internet-related services. The proposal does not require them to ascertain the original purpose for which the data were collected

by the users of the services.

28. It should be noted that this proposal not only seeks to regulate Internet or web-based data processors but also other outsourcing agents. An example is found in a real case where it was reported in the news that the contractor of a law enforcement agency did not properly shred confidential waste papers entrusted to them. Consequentially, the waste papers containing sensitive witness statements were sold as recycled paper.

29. Direct regulation on data processors and outsourcing activities will impose on the data processors concerned explicit obligations under the PDPO so that they will face regulation from the PCPD directly.

Harnessing Impact on Personal Data Privacy Caused by Technological Advancement

Proposal 38 – *More stringent regulation of Sensitive Personal Data*

30. The proposal to give recognition to specific categories of personal data as sensitive personal data is well recognized under the data protection laws in overseas jurisdictions. The overseas models (such as the *European Union Directive 95/46/EC,* the *UK Data Protection Act 1998*, the *Australian Privacy Act 1988*) also prohibit the collection, holding, processing and use of sensitive personal data except under prescribed circumstances.

31. Article 8 of the European Union Directive 95/46/EC Guidelines on the Protection of Privacy and Transborder Flow of Personal Data provides that "*Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.*" Also, the UK Data Protection Act has treated "*the commission or alleged commission of an offence and any proceedings relating to an offence alleged to have been committed*" as sensitive personal data. In its public consultation, the Administration has modified the PCPD's original proposal by singling out only biometric data as sensitive personal data as a start.

32. The proposal to give special treatment for sensitive personal data is in accord with Article 8 of the EU Directive 95/46/EC thereby enabling the PDPO to pass the EU adequacy test, namely it is a pre-requisite under the EU

Directive that member states must ensure similar level protection of personal data in the country to which the data will be transferred. Hence, adoption of the EU approach will enable uninterrupted exchange of personal data with the EU member states which is conducive to the sustained growth in trade and business activities in Hong Kong.

33. Special care is warranted in the handling of special categories of personal data in view of the gravity of harm that may be caused to the data subjects if such data are mishandled. With the eventual sharing of health data through the e-health programme, the implication is that huge amount of sensitive personal data of the general public will be centralized and made available to various data users. Also, the peril of sensitive personal data being mishandled is greatly increased as a result of technological enhancement (e.g. transmission through the Internet and storage of data by electronic means). The wide dissemination of the photos concerning the *sex life* of prominent artists a few years ago causing significant damage to the individuals concerned is a case in point. Measures should be taken now to give higher protection of sensitive personal data before another outbreak and community outcry.

34. Most of the views expressed in the Consultation Report agreed with the general direction of providing a higher degree of protection to sensitive personal data. The consultation has been focused on biometric data, to the neglect of other sensitive personal data. If the public could be invited again to give submissions on other types of personal data, the topic can be discussed in a thorough and more balanced manner, and the results would better meet the aspirations of the community.

Other Areas of Difference in Views

35. Further, the PCPD takes different views from the Administration on other proposals which are briefly set out in the Schedule for easy reference. The Schedule also sets out the major differences mentioned in the preceding paragraphs for completeness.

The Privacy Commissioner's appeal

36. The Privacy Commissioner urges the community to respond to the CMAB's invitation for views on the review of the PDPO and in light of this

PCPD submission.

37. The PDPO is enacted to protect the personal data privacy of individuals. It is now the general public's golden opportunity to voice their needs and preferences, so that the provisions of the PDPO could be brought in line with their expectations and international standards.

Office of the Privacy Commissioner for Personal Data
12 November 2010

Schedule

Table for Major Difference in Views

Personal Data (Privacy) Ordinance, Cap. 486 = "PDPO"
Office of the Privacy Commissioner for Personal Data = "PDPO"
Administrative Appeals Board = "AAB"
Data Protection Principles in Schedule 1 of the PDPO = "DPPs"
Government's Stance – Where it is stated "Partly Taken or Taken", it means the Government proposed to take forward or partly take forward the proposal.
– *Where it is stated "Not Taken", it means the Government proposed not to take forward the proposal.*
– Where it is stated "Proposal Not Pursued", it means the Government did not pursue the proposal in the Consultation Document.

Proposal No in Consultation Report	Name of Proposal (Government's Stance)	**Government's proposed way forward**	**PCPD's Views**
1	**Collection and Use of Personal Data in Direct Marketing** (Partly Taken)	- To increase the penalty level for misuse of personal data in direct marketing under s.34(1)(b)(ii). - To introduce specific requirements on data	- These requirements seems only apply where data users obtained personal data directly from data subjects but not from other source. Should consider PCPD's other

		user who intend to use personal data for Direct Marketing ("DM") purpose: (1) Reasonably specific Personal Information Collection Statement ("PICS") (i.e. classes of transferee, kinds of data, etc.); (2) Presentation of PICS (understandable, reasonably readable); (3) Option to choose not to agree to DM or transfer of personal data (bundled consent issue). - Not appropriate to: (1) pursue the "subscribe/ opt-in" proposal (reason: will add burden to operations of enterprises carrying out direct marketing activities); or (2) introduce a territory-wide do-not-call register against direct marketing activities (reason: it goes beyond the protection of personal data privacy).	proposals: "opt-in" regulatory regime, "do-not-call" register and right to data subject to request data user to disclose the source of personal data.
2	**Unauthorized Sale of Personal Data by Data user** (new)	- To introduce requirements in the PDPO to require a data user to comply with certain conditions if it is to *sell* personal data (whether collected from the data subject directly or obtained from other source) to	- The word *"sell"* should be given a wider definition to cover situation where data user merely *shared* the personal data with its business partners whether for monetary or

		another party for a monetary or in kind gain.	in-kind gain.
3	**Disclosure of Personal Data Obtained without the Data User's Consent for Profits or Malicious Purposes** (Partly Taken)	- To make it an offence for a person who discloses for "*profits or malicious purposes*" personal data which he obtained from a data user without the latter's consent.	- The Government should also look into providing civil remedies. PCPD takes the view that both criminal sanction and civil remedies (such as injunction order) should be provided. (Elaborated at the end of this Table*)
5	Regulation of Data Processors and Sub-contracting Activities (Partly Taken)	- To require data user to use contractual or other means to ensure that its data processors and any sub-contractors, whether within HK or offshore, comply with the requirements under the PDPO. - Not intend to impose direct regulation on data processors. The reasons are: - • data processors in Internet-related businesses do not have knowledge of the nature or use of the data and procedures involved in data processing are complicated and hence	- Indirect regulation means that the data processors will only be subject to civil sanction e.g. breach of contract or loss of business. Direct regulation on data processors is also necessary. - Justifications: - • many data leakage incidents show that the cause was the lack of security safeguards on the part of data processors; • *Google's Street View incident* illustrates the importance of

		the proposal may impede free flow of information on internet; and • encourage more data processors to get around the regulation by shifting work procedures to overseas and hence undermining competitiveness of HK.	strengthening regulations on Internet Service Providers (ISPs) and web-based services providers in respect of data privacy protection; • a data processor in Internet-related business is only required to ascertain the purpose for which the data were entrusted to it by the data user, but not the original purpose for which such data were collected; • requires data processor to comply with DPP 2(2) (retention), DPP 3 (use) and DPP 4 (security) only; • introduction of new obligations on data users in sub-contracting activities (using contractual or other means to ensure compliance by sub-contractors) should not obviate or substitute the need for direct regulation on data processors.
6	Personal Data Security	- To start with a voluntary privacy breach	- Should introduce mandatory data

	Breach Notification (Partly Taken)	notification system - Reasons: - • privacy breach notification system is not yet mature; and • onerous burden on data users.	breach notification in phrases. - Justifications: - • Mandatory data breach notification is the world trend, overseas examples: over 30 states of the US, Canada and also recent recommendation by the Australian Law Reform Commission to introduce mandatory system in Australia; • PCPD already issued "*Guidance on Data Breach Handling and the Giving of Breach Notification"* in June 2010 with a template of notification.
11	Additional Grounds for Refusing to Investigate (Partly Taken)	- Only to include the additional ground under s.39(2) that the cause of complaint is not related to personal data privacy.	- The following grounds should also be added to s.39(2), namely (i) the complaint relates to any action which is currently or soon to be under investigation by another regulatory body; and (ii) the complaint relates to documents

			which have been or will likely be or are intended to be used at any proceedings or inquiry. - Justifications: - • for ground (i) – avoid duplication of effort and the Ombudsman Ordinance contains similar provision (s. 10(1)(e)(ii)); and • for ground (ii) – avoid unnecessary appeals to AAB if PCPD can rely on this express provision other than the general ground under s.39(2)(d).
17	Power to Obtain Information to Verify a Data User Return (Taken)	- Proposal taken to ensure accuracy of a Data User Return	- The PCPD also proposed to be conferred with the power to specify, from time to time and by notice in the Gazette, the "prescribed information" to be reported in a data user return. - After *Octopus Card* incident, it is likely that the public will require for

			more details to be provided by data users in the data user return the use of personal data for direct marketing purposes and the relevant types of personal data transferred for those purposes.
18	**Repeated Contravention of a DPP on Same Facts** (Taken)	- Proposed that the penalty should be the same as that for breaching enforcement notice, i.e. liable to a fine at level 5 (HK$50,000) and imprisonment for two years upon conviction.	- Proposed higher penalty level taking into account the more culpable nature of repeated contraventions when compared with non-compliance of an enforcement notice. - Currently, under section 101E of the Criminal Procedure Ordinance Cap.221, a director or other officer of an organizational data user may be prosecuted and made guilty of the offence under the PDPO where it is proved that the offence was committed with the consent or connivance of a director or other officer concerned in the management of the company. In order to give a

			clear message to the public, it is further proposed to add a subsection to s. 64 of PDPO to the effect that a director or other officer of an organizational data user may be prosecuted and made guilty of the offence under the PDPO.
19	Repeated Non-compliance with Enforcement Notice (Taken)	- Proposed a fine (i.e. at Level 6 (HK$100,000) with same term of imprisonment (i.e. two years), and in the case of continuing offence, a daily fine of HK$2,000.	- Proposed higher penalty taking into account the more culpable nature of such offence with first-time non-compliance of an enforcement notice and the new offence of repeated contravention of a DPP on same facts under Proposal 18.
23	Response to Data Access Requests in Writing and Within 40 Days (Taken)	- To exempt the Police exclusively from the requirement of giving written response within 40 days after receipt of data access request for criminal conviction record if the requestor has a clear record.	- Exemption should not be granted lightly. The sole reason for allowing exclusion - “labeling effect”- does not provide sufficient justification and should, if it does exist, be more properly addressed by looking into the root of the problem, i.e. whether DPP1(1) has been breached by

			excessive collection of personal data.
30	Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship **(Taken)**	- This proposal was made by the Administration.	- There is no equivalent or similar exemption under overseas privacy legislations. - A better solution is to tackle the situation as identified in the proposal by way of other child protection laws. - Consideration should be given to the type of the exempted personal data, the degree of disclosure and the relevant circumstances at the material time. - A robust mechanism should be built in to guard against misuse. - Should consider allowing minors who attain certain age to make their own decisions in relation to the disclosure of the personal data.
35	Definition of Crime under s.58 (Taken)	- To add a definition of "crime" to ensure that law enforcement agencies under multilateral and bilateral cooperative	- Proposed that the draft definition should be confined narrowly according to s.5(1)(g) of the Mutual

		agreements or arrangements may provide personal data to their overseas counterparts for criminal investigations or detection of crimes overseas, and that assistance can be provided to foreign jurisdictions in verifying personal data in connection with requests for legal assistance.	Legal Assistance in Criminal Matters Ordinance (Cap. 525), which provides that the Secretary for Justice may refuse such request for legal assistance from overseas where the request relates to an act or omission that, if it had occurred in Hong Kong, would not have constituted a Hong Kong offence.
38	**Sensitive Personal Data** (Not Taken)	- Not intend to introduce a more stringent regulatory regime for sensitive personal data at this stage (because of no consensus on the coverage and regulatory model).	- Most of the views expressed in the Consultation Report agreed with the general direction of providing higher degree of protection to sensitive personal data. - Protection level of special categories of personal data should be brought at par with the standard stipulated in the EU Directive 95/46/EC. - The consultation should not be focused on biometric data. - The public should be consulted again.

39	Granting Criminal Investigation and Prosecution Power to the PCPD (Not Taken)	- Status quo should be maintained and the PCPD should not be given the power to investigate into and prosecute criminal offence cases.	- PCPD should be granted with criminal investigation and prosecution power, together with power to search and seize evidence and power to call upon public officers for assistance
Annex 5 Annex 5	**Power to Search and Seize Evidence** (Proposal Not Pursued) Power to Call upon Public Officers for Assistance (Proposal Not Pursued)	- Grounds for opposing the proposals: - • existing arrangements have worked well; • PCPD would have excessive power resulting in loss of checks and balances; • will give rise to conflict of interest as PCPD is the enforcement authority of the PDPO; • more appropriate for DOJ to follow up on prosecution; • confusion over PCPD's role; and • overlapping of structure and waste of resources.	- Grounds for supporting the proposals:- • speedy investigation as PCPD possesses first-hand information; • PCPD is proficient in interpreting and applying the provisions of PDPO; • save time on referring cases to Police; • avoid criticism of favouritism where Police or other Government departments are involved as data users; • avoid duplication of efforts of PCPD and Police; • will not prejudice Secretary for Justice's discretion to prosecute; and

			• number of cases for prosecution will increase substantially if new proposals are taken on board and with the various offences added.
40	Empowering the PCPD to award compensation to aggrieved data subjects (Not Taken)	- Not intend to implement this proposal. - Reason: in common law system, it is undesirable to vest in a single authority both the enforcement and punitive functions (LRC's view in "Report on Reform of the Law Relating to the Protection of Personal Data" ("LRC's Report") issued in August 1994 considered)	- Power under this proposal should be granted to the PCPD. - Justifications: - • Modeled on s.52 Privacy Act, Australia; • direct deterrent effect against infringement; • LRC's said view was premised on an assumption not existing under current provisions of PDPO.
42	Empowering the PCPD to Impose Monetary Penalty on Serious Contravention of Data Protection Principles	- Not intend to implement this proposal - Reasons: - • undesirable to vest in a single	- Power under this proposal should be granted to the PCPD. - The proposal is modeled on s.55 of the *Data Protection Act, UK*. The

	(Not Taken)	authority both the enforcement and punitive functions (LRC's view in LRC's Report considered); • under common law system, the roles of investigation, prosecution and adjudication should be performed by different institutions for checks and balances; and • more appropriate to specify serious contravention a criminal offence.	UK Information Commissioner also published a "*Guidance about the Issue of Monetary Penalties prepared and issued under s. 55C(1) of the Data Protection Act 1998*". - The power will greatly enhance the effectiveness of the PDPO and PCPD may impose sanction in appropriate case where serious contravention is involved. It will take long time for legislative amendment to make a specific contravention an offence.
44	**Fee Charging for Handling Data Access Request** (Not Taken)	- Not intend to implement this proposal - Reasons: - • difficult to prescribe appropriate and standardized levels of maximum fees for all chargeable items; and • not appropriate to include a fee schedule that requires adjustment from time to time.	- Proposal is to follow LRC's recommendation in LRC's Report. - Justifications: - • avoid unnecessary complaints if fees charged at the prescribed level; • chargeable items in the proposed fee schedule are not meant to be exhaustive.

Annex 5	**Territorial Scope of the PDPO** (Proposal not pursued)	- To provide that the PDPO does not apply to an act or a practice that the data processing cycle (i.e. the collection, holding, processing and use of which) occur *wholly* outside Hong Kong.	- For practical and other reasons, the mere presence in Hong Kong of a person who is able to control his business operations overseas should not render him a data user subject to Hong Kong law. It would be unfair to the person if the Hong Kong law and overseas law both govern the handling of the data not originated from Hong Kong, particularly where there is a conflict of laws situation. - The LRC report was prepared 15 years ago in 1994. Personal data privacy protection is an evolving concept in human rights and electronic trade and commerce and should be reviewed in light of the development in Hong Kong and overseas.
Annex 5	**Power to Conduct Hearing in Public**	- Not propose to change the current system	- Proposed that flexibility should be introduced to allow PCPD to decide

	(Proposal Not Pursued)	- Reasons: - • LRC considered that a public hearing could act as real disincentive to the lodging of complaint; and • PCPD's power to publish an investigation report under s. 48(2) of PDPO may take care of the public's right to know and be informed.	whether a hearing should be conducted in public having regard to all circumstances. - Justifications: - • public hearing with the complainant to remain anonymous can address LRC's concern; • *Octopus Card case* proved the effectiveness and resultant educational value of conducting public hearing.
Annex 5	Time Limit for Responding to PCPD's Investigation/ **<u>Inspection</u>** **(Proposal Not Pursued)**	- Not appropriate to take forward the proposal to shorten the time limit for responding to PCPD's investigation / inspection report (from 28 to 14 days) as it takes time to circulate report for comments and seek legal advice.	- With the rapid development in technology and telecommunication, the time limit should be reduced. - Especially, if the case involves serious public concern such as the *Octopus card* case.
***New (not proposed in**	Civil Remedy for Injunction Order	- N/A	- To address the concern whether civil remedy such as injunctive relief

the Consultation Report)			should be provided to data subject. - May make reference to the Australian Privacy Act 1988, by which the complainant or the Australian Privacy Commissioner may enforce a determination made by the Australian Commissioner for civil remedy including injunction order. - Civil remedy for injunction order is available under the Equal Opportunity Commission regime in Hong Kong.