PCPD's Submissions

To

Consultation Document on Review of the Personal Data (Privacy) Ordinance

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Contents:

		Page No.
I.	Purpose ……..…...	1
II.	PCPD's Response to the Consultation Document……...….....	2
	Sensitive Personal Data……...…..	**2**
	Proposal No. 1 : Sensitive Personal Data ……...….	2
	Data Security…….…….	**10**
	Proposal No. 2 : Regulation of Data Processors and Sub-contracting Activities …….	10
	Proposal No. 3 : Personal Data Security Breach Notification ……	16
	Enforcement Powers……...	**20**
	Proposal No. 4 : Granting Criminal Investigation and Prosecution Power to the PCPD …….....	20
	Power to Search and Seize Evidence	
	Power to Call Upon Public Officers for Assistance	
	Proposal No. 5 : Legal Assistance to Data Subjects under Section 66……...…….....	24
	Proposal No. 6 : Award Compensation to Aggrieved Data Subjects……...	24
	Offences and Sanctions……...	**27**
	Proposal No. 7 : Making Contravention of a Data Protection Principle an Offence ……..…	27
	Proposal No. 8 : Unauthorized Obtaining, Disclosure and Sale of Personal Data …….....	27
	Proposal No. 10 : Imposing Monetary Penalty on Serious Contravention of Data Protection Principles……..…….....	27

Proposal No. 9 : Repeated Contravention of a Data Protection Principle on Same Facts …….. 30

Proposal No. 11 : Repeated Non-compliance with Enforcement Notice ……..…. 30

Proposal No. 12 : Raising Penalty for Misuse of Personal Data in Direct Marketing ……...……... 31

Rights of Data Subjects……... 37

Proposal No. 13 : Third Party to Give Prescribed Consent to Change of Use of Personal Data……..... 37

Proposal No. 14 : Parents' Right to Access Personal Data of Minors……....… 43

Proposal No. 27 : Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship……... 45

Enhancing the Effectiveness of Ordinance…….…..... 47

Proposal No. 20 : Circumstances for Issue of an Enforcement Notice ……... 47

Proposal No. 21 : Clarifying Power to Direct Remedial Steps in an Enforcement Notice ……..... 53

Proposal No. 22 : Removing the Time Limit to Discontinue an Investigation…….……..... 53

Proposal No. 23 : Additional Grounds for Refusing to Investigate …….. 54

Annex 2 to the Consultation Document – Proposals Not to be Pursued……...…...…. 60

Revamping Regulatory Regime of Direct Marketing……... 60

Internet Protocol Address as Personal Data…….. 63

Territorial Scope of the Ordinance…… 65

Public Interest Determination…….…..… 68

Public Domain Exemption……...… 71

Power to Search and Seize Evidence…… 72

Power to Call Upon Public Officers for Assistance…….. 72

Power to Conduct Hearing in Public……..…….. 72

Time Limit for Responding to PCPD's Investigation/Inspection Report……...……. 73

Annex 3 to the Consultation Document – Miscellaneous Proposed Amendments to the Ordinance……. 74

Proposal No. 32 : Power to Obtain Information to Verify a Data User Return…….……..... 74

Proposal No. 36 : Definition of Crime under Section 58…... 75

Other Proposals……...……... 78

III. Schedule……...……....…... 79

I. Purpose

1.1 On 28 August 2009, the Constitutional and Mainland Affairs Bureau (CMAB) released the Consultation Document on Review of the Personal Data (Privacy) Ordinance ("the Ordinance").

1.2 The review was initiated by the Privacy Commissioner for Personal Data (PCPD) in June 2006. An internal Ordinance Review Working Group was formed to assess the adequacy of protection of personal data privacy. After a year and a half's work, the Working Group completed its review and presented to the Government in December 2007 more than 50 amendment proposals and issues of privacy concern.

1.3 The Government has taken on board most of the proposals made by the PCPD. In order to let the public know more about the issues before making their submissions, the PCPD published a paper entitled "PCPD's Information Paper on Review of the Personal Data (Privacy) Ordinance" ("the Information Paper") on 9 September 2009. The Information Paper has been uploaded to PCPD's web-site[1].

1.4 This Submission sets out PCPD's response to various amendment proposals made in the Consultation Document. Where appropriate, specific references are made to the relevant materials contained in the Information Paper. In reading this Submission, readers are strongly encouraged to refer to the Information Paper for background materials.

Office of the Privacy Commissioner for Personal Data
November 2009

[1] http://www.pcpd.org.hk/english/review_ordinance/files/Odnreview_Information_Paper_e.pdf.

II. PCPD's Response to the Consultation Document

2.1 Most of the proposals as set out in the Consultation Document had its origin in PCPD's 2007's proposals to the Government, which were intended to afford greater protection to personal data privacy. The Government's proposals even though more moderate and conservative than those made by the PCPD should still on the whole achieve the same objective. Some of these proposals deal with matters of significant privacy impact while others seek to strengthen the enforcement power of the PCPD and improve the efficacy of the regulation of the Ordinance. New mechanisms to deal with issues of public concern are also introduced. All these aim at bringing about an update piece of legislation that best suits the public in the protection of personal data privacy.

Sensitive Personal Data

Proposal No. 1 : Sensitive Personal Data

2.2 This proposal was originally made by the PCPD[2] to prohibit the collection, holding, processing and use of specific categories of personal data (to be defined as sensitive personal data) except under prescribed circumstances. The Administration has modified PCPD's original proposal by singling out only biometric data as sensitive personal data as a start.

Whether there is a need to accord better protection to sensitive personal data

2.3 Amending the Ordinance to give special treatment for sensitive personal data is in accord with Article 8 of the EU Directive 95/46/EC *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* thereby enabling the Ordinance to pass the EU adequacy test. It is a pre-requisite under the EU Directive that member states must ensure similar level of 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

[2] See PCPD's Proposal No. 1 at p.1 in the Annex to the Information Paper.

states. This is conducive to Hong Kong's prosperous growth in trade and business activities.

2.4 The PCPD therefore recommends that the protection level of special categories of personal data should be brought at par with the standard stipulated in the EU Directive 95/46/EC.

Coverage of sensitive personal data

2.5 Article 8 of the EU Directive 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."

2.6 The PCPD recommends the adoption of the categories specified in Article 8 with modifications. The PCPD suggests that "political opinion" and "religious or philosophical beliefs" be replaced by "political affiliation" and "religious beliefs and affiliations" respectively.

2.7 The PCPD is of the view that special care is warranted in the handling of special categories of personal data in view of the gravity of harm that may cause the data subjects if such data are mishandled. In anticipation of the eventual implementation of electronic health record sharing system where massive sensitive health records are kept in databases for use and access, the PCPD considers that more stringent control and prudent practice are required in relation to the handling of medical data.

2.8 The PCPD also supports the inclusion of biometric data as sensitive personal data. Biometric data can be considered sensitive since they are fixed and, unlike a password or a PIN, cannot be reset once they have been inappropriately released. They are very personal and private because they are information about an individual's physical self. Biometric data, such as fingerprints and genetic data, should be accorded higher protection. Biometric technologies, such as facial recognition technologies, may be used to identify individuals without their knowledge or consent, and that biometric data could reveal other sensitive personal information, such as information about a person's health, racial or ethnic origin or religious beliefs. They can provide the

basis for unjustified discrimination.

2.9 Recently, as a result of advancement in technology, there has been a proliferation in the use of biometric devices, such as fingerprint scanners, for identification/verification purpose. In such a system, a biometric sample is taken from an individual. Data from the sample are then analyzed and converted into a biometric template, which is stored in a database or an object in the individual's possession, such as a smart card. Later, biometric samples taken from the individual can be compared to the stored biometric template to identify the individual or to verify the individual's identity.

2.10 In July 2009, the PCPD published a report[3] concerning the collection and recording of employees' fingerprint data for attendance purpose by a furniture company. In that case, the PCPD found that the collection of employees' fingerprint data by the company for monitoring attendance purpose was excessive and the means of collection was not fair in the circumstances of the case and consequently the company's practice was in contravention of Data Protection Principle ("DPP") 1(1) and DPP1(2) in Schedule 1 of the Ordinance.

2.11 In the light of the experience in handling complaints lodged with the PCPD involving the collection of personal data by fingerprint scanners, the PCPD arrived at the following general views:-

(a) First and foremost, if the act does not involve the collection of "personal data", it is outside the jurisdiction of the Ordinance. For example, there is a fingerprint recognition system that can convert certain features of the fingerprint into a unique value and store it in the smart card held by the employee (the employer does not hold a copy of the data). For verification, the employee needs to put his finger and the smart card on the recognition device. The system merely compares and matches the value in the smart card with the fingerprint features presented each time and the employer has no access to the personal data concerned. As the employer has not collected employees' fingerprint data or their value, he has not collected any "personal data" as defined in

[3] Available at http://www.pcpd.org.hk/english/publications/files/report_Fingerprint_e.pdf

the Ordinance;

(b) If the fingerprint recognition system involves the collection of personal data, employers should be mindful not to collect fingerprint data purely for attendance purpose. In many other instances, there exist less privacy intrusive alternatives which can achieve the purpose of monitoring attendances. Whether or not features of the fingerprints are converted into value, such an act amounts to collection of excessive personal data and contravenes the requirements of DPP1(1), unless the genuine consent of the data subject has been obtained;

(c) If a data subject provides his fingerprint data voluntarily for a particular purpose, the application of the DPPs should not override the data subject's right to information self-determination. The PCPD will respect his consent if given voluntarily and explicitly;

(d) Fingerprint data should not be collected from children of tender age, regardless of any consent given by them, for reason that they may not fully appreciate the data privacy risks involved;

(e) Before collecting employees' fingerprint data for attendance purpose, employers must offer employees a free choice in providing their fingerprint data, and they must be informed of the purpose of collection and given other less privacy intrusive options (e.g. using smart cards or passwords);

(f) The means of collecting employees' fingerprint data must be fair. Employees should be able to give their consent voluntarily without undue pressure from the employers and should have the choice of other options; otherwise there may be contravention of the requirements of DPP1(1) and DPP1(2).

2.12 There are arguments that the data stored in a fingerprint recognition system are not personal data because:-

(a) the stored biometric data are just meaningless numbers, and

therefore are not personally identifiable information; and

(b) a biometric image cannot be reconstructed from the stored biometric template.

2.13 In relation to the argument in 2.12(a), while the numbers may not be able to identify an individual when considered alone, they are capable of identifying an individual when linked to other personal identification particulars. Similar examples are identity card numbers, credit card numbers and mobile phone numbers. The purpose of a fingerprint recognition system is to identify or verify the identity of an individual. The templates will ultimately be linked to identify a person. Hence, no matter how the templates are generated (in the form of numerical codes or otherwise), they will be considered "personal data" when combined with other identifying particulars of a data subject.

2.14 With respect to the claim that a fingerprint image cannot be reconstructed from the stored biometric template, Information and Privacy Commissioner of Ontario states in a paper entitled "Fingerprint Biometrics: Address Privacy Before Deployment"[4] issued in November 2008 the different view taken in some recent scientific works[5]:-

> *"Until recently, the view of non-reconstruction was dominant in the biometrics community. However, over the last few years, several scientific works were published that showed that a fingerprint can, in fact, be reconstructed from a minutiae template. The most advanced work was published in 2007 by Cappelli et al. The authors analyzed templates compatible with the ISO/IEC 19794-2 minutiae standard. In one test, they used basic minutiae information only (i.e. positions x, positions y, and directions). In another test, they also used optional information: minutiae types, Core and Delta data, and proprietary data (the ridge orientation field in this case). In all the tests, the authors were able to reconstruct a fingerprint image from the minutiae template. Very often, the reconstructed image had a striking resemblance with the original image. Even though this reconstruction was only*

[4] Available at http://www.ipc.on.ca/images/Resources/fingerprint-biosys-priv.pdf
[5] See p.7 of the paper

approximate, the reconstructed image was sufficient to obtain a positive match in more than 90% of cases for most minutiae matchers."

2.15 The paper goes on to discuss the potential repercussions for security and privacy of fingerprint minutiae systems:-

"The potential repercussions of this work for the security and privacy of fingerprint minutiae systems are as follows:

The fingerprint image reconstructed from the minutiae template, known as a "masquerade" image since it is not an exact copy of the original image, will likely fool the system if it is submitted.

A masquerade image can be submitted to the system by injecting it in a digital form after the fingerprint sensor.

A malicious agent could also create a fake fingerprint and physically submit it to the sensor. The techniques of creating a fake fingerprint are inexpensive and well-known from the literature.

The ability to create a masquerade image will increase the level of interoperability for the minutiae template. The masquerade image can be submitted to any other fingerprint system that requires an image (rather than a minutiae template) as an input. No format conversion of the minutiae template would be required. Moreover, the minutiae template can be made compatible even with a non-minutiae fingerprint system (these systems are rare, however)."

2.16 The Australian Law Reform Commission ("ALRC") sees the need of extending the definition of "sensitive personal data" to cover biometric information. The ALRC made the proposal in its Report 108 – For Your Information: Australian Privacy Law and Practice[6] issued in August 2008. In recognizing that requiring consent to collect all

[6] Available at http://www.austlii.edu.au/au/other/alrc/publications/reports/108/6.html#Heading283

biometric information may be impracticable, the ALRC recommended to amend the Privacy Act to include the following in the definition of "sensitive personal data":-

(a) biometric information collected for the purpose of automated biometric verification or identification; and
(b) biometric template information.

2.17 The above are regarded as the most serious privacy concerns around the handling of biometric information and the recommendation is intended to address such concerns.

2.18 In October 2009, the Australian Government released its first stage response to the ALRC report[7]. The Australian Government recognized the importance of attributing a higher level of protection to personal information which is sensitive in nature and agreed that biometric information has similar attributes to other sensitive information and it is desirable to provide it with a higher level of protection. Given the broad nature of what can be considered biometric information, the Australian Government considered that the definition should make clear that the additional protections should only extend to that biometric information which is specifically being collected to identify or verify an individual through biometric processes.

Requirements in handling sensitive personal data

2.19 The PCPD supports the proposed exceptions to special treatment of sensitive personal data as stipulated in paragraph 3.09 of the Consultation Document.

Sanction for contravention of requirements

2.20 In view of the sensitive nature of the data and the degree of harm that could result in mishandling the data, a more stringent control should be imposed. The PCPD supports the proposal to make it an offence for any person who without reasonable excuse, fails to comply with the prescribed requirements governing the handling of sensitive personal

[7] Available at http://www.pmc.gov.au/privacy/alrc.cfm

data. Since the proposed provision is new to the public, the PCPD suggests that any penalty should be restricted to the imposition of a fine but not a custodial sentence.

Grandfathering

2.21 The PCPD considers that a data user, who has collected any sensitive personal data before the commencement date of the new requirements, may continue to hold the data already collected. However, any subsequent use of the data should follow the new requirement by seeking the prescribed consent of the data subject.

2.22 To enable the public to become familiarized with the new requirements, the PCPD supports a transitional period for the implementation of the new requirements. It should however be borne in mind that fixing an unduly long transitional period will defeat the purpose of putting in place the new protection to sensitive personal data. The PCPD takes the view that the transitional period to be imposed should not be longer than twelve months.

Other comments

2.23 The PCPD urges the Government to reconsider its decision to single out biometric data from the seven types of "sensitive personal data" suggested by the PCPD. In particular, the PCPD asks the Government to seriously consider the inclusion of a person's physical and mental health condition as "sensitive personal data".

Data Security

3.1 With the rapid development of technology, the storage and disclosure of personal data often raise privacy concerns. Measures to ensure sufficient control and security are necessary in view of the increase of data losses and leakage incidents.

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

Whether a data user should be required to use contractual or other measures to secure its data processor's compliance with the relevant obligations under the Ordinance

3.2 This proposal was originally made by the PCPD[8] to the Administration. It is proposed to impose specific obligations on a data user, who transfers personal data to a data processor for holding, processing or use, to employ contractual or other means to require its data processor and any sub-contractors to take all practicable steps to ensure the security and safekeeping of the data, and to ensure that the data are not misused and are deleted when no longer required.

3.3 The PCPD expects a data user, in order to comply with the proposed specific obligation, to select a contractor of reasonable standard and quality that can provide adequate security of the personal data. The terms of the service agreement shall include the following provisions:-

(a) prohibition against any use or disclosure of the personal data by the contractor for a purpose other than the purpose for which the personal data are entrusted to it by the data user;

(b) security measures required to be taken by the contractor to protect the personal data entrusted to it, including imposing contractual obligations on the contractor to comply with the data protection principles of the Ordinance;

(c) timely return or destruction of the personal data when they are no

[8] See PCPD's Proposal No. 2 at p.8 in the Annex to the Information Paper.

longer required for the purpose for which they are entrusted by the data user to the contractor;

(d) absolute or qualified prohibition on the contractor against sub-contracting the service;

(e) immediate reporting of any sign of abnormalities or security breaches by the contractor; and

(f) measures required to be taken by the contractor to ensure that its relevant staff will carry out the security measures and comply with the obligations under the service agreement regarding the handling of personal data.

3.4 It is normal business practice for a data user to enter into a contractual relationship with its data processors. Introduction of specific obligations on organizations to enter into the contractual terms for the protection of personal data with their contractors should not disrupt normal business activities. The contract may serve as evidence to show the data user's compliance with the requirements of the Ordinance in case a complaint is brought by a data subject against the data user for infringement of personal data privacy in relation to the act or practice of its data processing agent.[9]

3.5 It is important to note that the contractual requirement above is insufficient to effectively regulate the activities of the data processors. While the data processors may be liable to the data users under their contracts, their conduct may not be regulated by the Ordinance.

Direct or indirect regulation on data processors

3.6 It is unsatisfactory that the Ordinance does not regulate the handling of personal data by data processors as the definition of "data user" does not apply to them pursuant to section 2(12)[10]. Some of the data leakage

---

[9] A data user may be liable for any acts done by its agent by virtue of section 65 of the Ordinance. According to section 65(2), any act done or practice engaged in by a person as agent for another person with the authority (whether express or implied, and whether precedent or subsequent) of that other person shall be treated as done or engaged in by that other person as well as by him.

[10] Section 2(12) of the Ordinance provides "*A person is not a data user in relation to any personal*

incidents show that very often the cause of the incidents was the lack of sufficient security safeguards on the part of the data processors[11]. Therefore, the PCPD finds that direct regulation on data processors is essential.

3.7 Paragraph 4.13 of the Consultation Document asserts the difficulties in defining the generic obligations for data processors because many Internet-related businesses will be unaware of the nature of the data, including the purpose for which they were originally collected. The PCPD wishes to point out that the proposal only requires these Internet-related businesses 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.

3.8 The PCPD considers that, since the Internet-related businesses obtain personal data in the course of their business activities, the use of the personal data so obtained should be confined to the purpose of provision of the Internet-related services. Any use other than the original or a directly related purpose should be prohibited. To use the example of a social networking site given in paragraph 4.13 of the Consultation Document, the purpose for which any personal data were entrusted to the provider of the social networking site by its users should be the facilitation of the social networking. The provider does not have to ascertain the original purpose for which the users collected the personal data, even though the users may have posted up personal data in the social networking site for a different purpose.

3.9 The PCPD considers that the misunderstanding may be addressed by making appropriate amendments and/or additions to DPP3, so that the expression *"the purpose for which data were to be used at the time of collection"* in DPP3(a), in so far as it applies to the data processors, shall mean *"the purpose for which the data were entrusted to the data processor"*. The PCPD stresses that the concern can be addressed by

---

data which the person holds, processes or uses solely on behalf of another person if, but only if, that the first-mentioned person does not hold, process or use, as the case may be, those data for any of his own purposes".

[11] See PCPD's investigation report on the Independent Police Complaints Council, available at (http://www.pcpd.org.hk/english/publications/files/IPCC_e.pdf).

appropriate drafting of the amendments to the Ordinance instead of rejecting the whole idea of direct regulation.

3.10 Paragraph 4.15 of the Consultation Document also raises concerns that ISPs and web-based service providers might have problem to comply with the relevant DPPs as typically they have no knowledge of whether the data they are holding are personal data. The PCPD appreciates that inspection of each piece of communication processed by ISPs and web-based service providers may be technically and/or practically impossible. On the other hand, it is inevitable that personal data are being transmitted in those communication, and the risk of any data privacy breach on the part of the ISPs and web-based service providers is not merely hypothetical or remote.

3.11 The PCPD is of the view that the ISPs and web-based service providers are not required to examine each piece of information they process in order to find out whether it contains personal data, what kind of personal data they are, and to provide tailor-made security measures for each set of personal data. As responsible and prudent ISPs and web-based service providers, they should treat the information they obtained in the provision of the relevant services as containing "personal data". Similar to the example of a social networking site as discussed above, the purpose for which any personal data were entrusted to the ISPs and web-based service providers by their users should be the facilitation of the services, e.g. transmission of emails, rather than the purpose for which the users collected the personal data. As such, the ISPs and web-based service providers should be able to ascertain their obligations under the Ordinance, such as the restrictions on further use of the data, adequacy of data security, duration of data retention, etc.

3.12 Paragraph 4.16 of the Consultation Document raises a concern about uncertainty. It gives an example of an advertising-funded webmail provider who might transmit personal data on behalf of the sender, store, forward and index personal data on behalf of the recipient and process the data on behalf of third parties for the purpose of targeting marketing messages. It seems the concern is that the ISP is uncertain as to whether it has to consider the purpose for which the personal data were entrusted by the sender or the purpose for which they were entrusted by

the webmail provider. The PCPD appreciates that, like a data user, a data processor may process the same piece of personal data for multiple purposes. As far as the ISP is concerned, the entrusting of the personal data contained in an email by the sender and that by the webmail provider should take place within a split second. Besides, the purposes for which the data were entrusted by the sender and the webmail provider should be the same, i.e. transmitting the email to the recipients for the sender. As such, the ISP should have no practical difficulties in ascertaining the purpose for which the personal data are entrusted to it. To comply with the proposed obligations, the ISP shall not use the personal data for any purpose other than for the purpose of transmission and should erase the personal data after the transmission unless it has an obligation to retain the data.

3.13 Paragraph 4.17 of the Consultation Document raises a concern that many Internet-related businesses whose business purpose is to facilitate access to data, e.g. a search engine that caches data, may be left uncertain as to what constitutes unauthorized access to personal data. In the example, it seems that the provider of the search engine, which only caches data on its own initiative, is not entrusted with any personal data, hence, should not fall within the definition of "data processor." Additionally, in the PCPD's view, the requirement of DPP4 provides for safeguard of personal data against unauthorized or accidental access, etc. in the course of their transmission or storage. The example of a search engine should not be a matter of concern under DPP4 because access to the information or data concerned is authorized by the search engine.

3.14 The PCPD believes that paragraphs 3.8 and 3.9 above have also addressed the concern raised in paragraph 4.18 of the Consultation Document.

What obligations should be imposed on data processors?

3.15 The PCPD supports the option stated in paragraph 4.14 of the Consultation Document to require the data processors 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.

Whether it is appropriate and practical to subject different categories of data processors to different obligations

3.16 Paragraph 4.19 of the Consultation Document mentions that the Internet environment is fast-evolving and it is important that privacy laws do not inhibit the development of desirable new Internet-related services. It is suggested that, instead of directly regulating data processors in the field of Internet-related business, their obligations should be limited to adoption and observance of their own privacy policy relating to the use, security and retention of personal data, and any failure to observe the policy will be subject to the PCPD's enforcement action. In PCPD's view, data protection does not depend solely on the formulation of a comprehensive privacy policy. Besides, it is the statutory obligation of the PCPD to monitor and supervise compliance with the Ordinance. In discharge of his statutory obligation, the PCPD shall not solely rely on the discipline and good governance of the data processors and enforce the terms of the privacy policies dictated by the data processors. The PCPD is still unable to see a convincing justification for relaxing the requirements of data processors for Internet-related businesses exclusively.

3.17 It must be stressed that the introduction of obligations on the data users in sub-contracting activities should not obviate or substitute the need for those obligations proposed for the data processors. These obligations are separate and essential to ensure protection at all levels. The PCPD does not consider it sufficient protection for the public in relation to their personal data to simply rely on data users to regulate their contractors because the existing section 65(2) of the Ordinance already provides that a principal can be liable for the act of its agent. The gravity and recurrence of data leakage incidents have shown that direct regulation on

the data processors may be more effective to curb data leakage incidents by data processors.

Proposal No. 3 : Personal Data Security Breach Notification

3.18 This proposal was originally made by the PCPD[12] in responding to the series of personal data losses and leakage incidents which arouse grave public concerns. The PCPD supports the proposal that data users should be required to give security breach notifications in certain situations. The Administration considers it more prudent to start with a voluntary breach notification system so that they 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.

3.19 The PCPD observes that agencies and organizations are storing increasingly vast amounts of personal data electronically, some of which are sensitive in nature. The leakage of such data may allow identity theft of the affected individuals. It is evident that electronic leakage of personal data, e.g. through the Internet, is difficult, if not impossible, to contain. By the time a complaint is made to the PCPD, the personal data could have been downloaded and retained by countless unauthorized users on the Internet. Therefore, an early response to data leakage is crucial for protecting electronically stored personal data.

3.20 In the circumstances, serious consideration should be given to a containment plan which data users are required to adopt in order to mitigate or reduce the damages that may cause to the data subjects. Apart from other remedial measures, data users should be required under certain circumstances to notify the affected individuals of the security breach as soon as practicable after occurrence of the breach. This enables the affected individuals to take steps to prevent misuse of their personal data.

3.21 Security breach notification may not have a direct effect in preventing data leakage, it minimizes the exposure of the data subjects to possible

[12] See PCPD's Proposal No. 51 at p.136 in the Annex to the Information Paper.

damage. This is particularly so when a significant number of data subjects are affected by the breach and where sensitive personal data are lost or stolen. The Independent Police Complaints Council (IPCC) data leakage incident[13] is a good example where sensitive personal data were leaked on the Internet and the affected individuals have to be notified in order that they may take steps to prevent any misuse of their personal data. In that case, the IPCC gave the notification voluntarily.

3.22 The PCPD has received data users' voluntary notifications from time to time. During the period from 1 April 2008 to 31 July 2009, the PCPD received a total of 44 data breach notifications from data users in both private and public sectors. Concerning Government departments and public bodies, for the aforesaid 16 months period, the PCPD has received 33 incidents of security breach covering in total personal data of 16,303 individuals.

3.23 After receiving a notification of security breach, the PCPD will carry out a compliance check by enquiring with the relevant data users, pointing out the apparent insufficiencies in their data security system and inviting the data users, where appropriate, to take remedial actions. In many cases, the data users take the initiative and respond by undertaking immediate actions to remedy the data security breach. In other instances, the data users seek guidance and directions from the PCPD to step up security measures so as to avoid repetition of similar incidents in future.

3.24 To illustrate how PCPD reacts, below is a compliance check case which was prompted by a security breach notification:

> *The data user in this case is an insurance company in Hong Kong. By its letter of September 2008, the company informed the PCPD that an electronic file containing personal data of over 1,000 customers had been wrongfully sent to an unintended recipient by email. The company had contacted the wrong recipient who confirmed that the file had been deleted. The staff responsible for the wrongful dispatch*

[13] PCPD's investigation report available at http://www.pcpd.org.hk/english/publications/files/IPCC_e.pdf

was given a written warning.

In response to the compliance check initiated by the PCPD, the company formulated an action plan to strengthen the data transmission security by password protection, file automation and encryption. The company also informed the PCPD that its audit department would conduct a special review of the company's data transmission process focusing on data privacy.

In October 2008, the company provided a written undertaking to the PCPD agreeing to step up measures in respect of the security of the personal data held by it and provide the PCPD with a copy of its internal audit report on data transmission process.

3.25 Although many overseas jurisdictions have not made data breach notification a mandatory requirement, their privacy reforms all call for adopting a mandatory approach. Locally, the frequently reported incidents of data losses, particularly associated with the widespread use of portable electronic devices, call for tighter control. In addition, the feedback obtained from the recent consultative activities suggests solid support to making it a mandatory requirement.

3.26 The Government has already put in place a voluntary notification mechanism for personal data leakage incidents for a period of time. In view of the vast amount of personal data being held by the public sector and having regard to the expectation from the community, it will be desirable to impose mandatory breach notification on the public sector as a start.

3.27 There are concerns that it may cause the private sector undue burden to comply with the proposed requirements. It should be noted that under the proposed mechanism, a data user is not required to notify every security breach. It is only in those cases where the security breach may result in high risk of significant harm to individuals or organizations that notification is required. The PCPD will issue guidelines on the circumstances that would trigger the notification as well as the

particulars to be contained in the notice.

3.28 To facilitate smooth implementation of security breach notification, the PCPD recommends that, similar to data user return, the PCPD should be given the power to specify by notice in the Gazette the class of data users to which the notification requirement applies. In making the determination, the PCPD may consider a number of factors including the amount of personal data held by the specific class of data user, the degree of sensitivity of the data as well as the risk harm to the data subjects as a result of a security breach. The proposed mechanism ensures a gradual process and a selective approach that will balance different interests within the community.

Enforcement Powers

4.1 In order to strengthen the enforcement powers of the PCPD, various proposals were made by the PCPD to the Government. The purpose of the below proposals was to enhance efficiency of enforcement and to cause deterrence to infringements of the Ordinance.

Proposal No. 4 : Granting Criminal Investigation and Prosecution Power to the PCPD
Power to Search and Seize Evidence (C.1 of Annex 2 to the Consultation Document)
Power to Call Upon Public Officers for Assistance (C.2 of Annex 2 to the Consultation Document)

4.2 These proposals were originally made by the PCPD.[14] The PCPD advocated that specific power be conferred on the PCPD to carry out criminal investigation and prosecution. The power to search and seize evidence and to call upon public officers for assistance are incidental powers necessary for facilitating criminal investigation.

4.3 Paragraph 5.03 of the Consultation Document mentions three grounds which PCPD has put forward to support the proposal of granting PCPD prosecution powers. They are:-

(a) the PCPD possesses first-hand information obtained in the course of its investigations and can investigate into suspected commission of an offence speedily;

(b) as the regulator, the PCPD is proficient in interpreting and applying the provisions of the Ordinance, and can assess the weight and relevance of the evidence in any given situation with ease and confidence; and

(c) to save time on referring cases to the Police, hence to help meet the statutory time limit to lay prosecution which is set at six months from commission of an offence.

---

[14] See PCPD's Proposal Nos. 8, 14 and 16 at p.27, 44 and 48 in the Annex to the Information Paper.

4.4 Apart from the above reasons, granting prosecution power to the PCPD will help avoid criticism of favouritism where the Police or other government departments are involved in the case as data user. In addition, it will avoid the duplication of efforts of the PCPD and the Police. It is because usually the PCPD will carry out preliminary enquiries such as taking a statement from the complainant in order to satisfy that there is a *prima facie* case of commission of an offence before referring the complaint to the Police for criminal investigation. When the Police take over the case, they will take statement from the complainant again. The duplication of effort is a waste of both time and resources.

4.5 The Consultation Document states at paragraph 5.06 that there could be "community concerns" if prosecution power is delegated to the PCPD. However, there is no further elaboration as to what those concerns were. On the other hand, there are many examples where statutory bodies are empowered to carry out investigations and institute prosecutions on their own, such as, the Vocational Training Council, the Employment Compensation Assistance Fund Board, the Construction Workers Registration Authority and the Security and Futures Commission (paragraph 5.05 of the Consultation Document refers).

4.6 The power and function of prosecution entail the due presentation of facts to the Court. It does not place the PCPD in a position to decide or judge the culpability of any data user. That power is, as always, reserved for the judiciary.

4.7 The PCPD does not agree with the statement in paragraph 5.08 of the Consultation Document that *"whether the PDPO can afford effective protection to personal data privacy hinges on the adequacy of penalty sanction, rather than on who the party responsible for initiating prosecution is."* In PCPD's view, effectiveness in investigation and prosecution process is also an important contributing factor to the enforcement of the Ordinance. While the Administration states that it has put forth in Chapter Six of the Consultation Document proposals to step up the sanctions provided for in the Ordinance, it is noted that of the six proposals made in Chapter Six, the Administration has not shown

support to four of them[15].

4.8 Paragraph 5.04 of the Consultation Document mentions that strong justifications are required for the prerogative of initiating criminal prosecution to be delegated to the PCPD. In this respect, it should be borne in mind that a member of the community has the common law right to prosecute an offence. A feature of the early common law was the notion that it was not only the privilege but also the duty of the citizen to preserve the king's peace and to bring offenders to justice. Hence, under the common law every citizen has exactly the same right to institute any criminal prosecution as the Secretary for Justice or anyone else, although section 14 of the Magistrates Ordinance empowers the Secretary of Justice to intervene and assume the conduct of the proceedings at any stage of the proceedings before the magistrate.

4.9 The PCPD's proposal will not prejudice the Secretary of Justice's discretion to prosecute. It is because the granting of prosecution power to the PCPD entails only the carrying out of the prosecution work and the discretion whether or not to prosecute is always reserved for the Secretary for Justice. It will be made explicit in the law that the PCPD's power to prosecute shall be subject to the consent of the Secretary for Justice.

4.10 It has also been raised that the low number of referrals and successful convictions in the past years 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 after the referral. As for the number of referrals, the figures are 8, 9 and 5 for the years 2006, 2007 and 2008 respectively.[16] It rises to 9 cases in 2009 (as at 5.11.09). The following reasons may account for the low figures of referrals and prosecutions:-

(a) Many complaints are lodged after the time bar for prosecution

---

[15] The proposals not supported by the Administration are Proposal No. 7 (Making Contravention of a Data Protection Principle an Offence), Proposal No. 9 (Repeated Contravention of a Data Protection Principle on Same Facts), Proposal No.10 (Imposing Monetary Penalty on Serious Contravention of Data Protection Principles) and Proposal No. 11 (Repeated Non-compliance with Enforcement Notice).

[16] Paragraph 2.11 of the Consultation Document.

which is prescribed under the Magistrates Ordinance as six months[17];

(b) The complainants prefer the cases to be handled by the PCPD rather than the Police. It is the policy of the PCPD that consent should be sought from the complainant before any referral is made to the Police; and

(c) Cases of infringement of the Ordinance are generally not considered a priority in the array of offences within the purview of the Police both in terms of seriousness and urgency.

4.11 On the other hand, there is a strong likelihood that if the following proposals put forth by the PCPD are taken on board by the Administration, the number of cases for prosecution will increase significantly:-

(a) The proposal to extend the time limit for laying information for prosecution from 6 months to 2 years will certainly increase the number of cases suitable for prosecution;

(b) The proposal to widen the discretion of the PCPD to issue enforcement notices will certainly result in an increase in the issuance of enforcement notices, the breach of which is an offence;

(c) The proposals to create the following new offences will result in an increase in the number of cases for prosecution:-

(i) Contravention against the new provision for dealing with "sensitive personal data" (Proposal No. 1);
(ii) Knowingly or recklessly obtaining personal data without consent from the data user and the disclosure or sale of the data so obtained to third parties (Proposal No. 8);
(iii) Repeated contraventions of the Ordinance on the same facts where the first infringement has resulted in the issuance of an Enforcement Notice (Proposal No. 9);
(iv) Contravention against the requirement for

[17] Section 26 of the Magistrates Ordinance

destroy/return/use of data under the new "mergers, acquisition and transfer of business" exemption under Part VIII (Proposal No. 24).

Proposal No. 5 (Legal Assistance to Data Subjects under Section 66)
Proposal No. 6 (Award Compensation to Aggrieved Data Subjects)

4.12 These two proposals were originally made by the PCPD[18] in order to assist aggrieved data subjects to obtain compensation from the data users for any damages suffered by reason of the latter's infringement of the requirements of the Ordinance.

4.13 Paragraph 5.18 of the Consultation Document states that the LRC Report had thoroughly discussed the appropriate body to determine compensation under the Ordinance and 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. Also, it is not appropriate to adopt the Australian model which advocates settlement by conciliation. The power to determine the amount of compensation is part and parcel of the investigation power of the Australian Privacy Commissioner. Besides, there has already been put forth proposal No. 5 to assist aggrieved data subjects in seeking redress through civil remedy.

4.14 The PCPD would like to point out that the LRC's recommendation at that time was premised on the assumption that the Court would determine the appropriate amount of compensation upon the PCPD's certificate of contravention but ultimately no such arrangement has been introduced under the current provisions.[19]

4.15 Under the Australian Privacy Act, if conciliation fails to resolve a complaint, the Australian Privacy Commissioner may make a determination. In the determination, the Australian Privacy Commissioner may (a) make a declaration directing the respondent to take steps remedying the contravention; and (b) award damages to the

---

[18] See PCPD's proposals Nos. 54 and 53 at p.142 and 144 in the Annex to the Information Paper.

[19] See paragraph 16.72 of the Law Reform Commission Report on Reform of the Law Relating to the Protection of Personal Data issued in August 1995.

complainant. The PCPD may carry out the similar settlement by conciliation. Indeed, many of the cases handled by the PCPD are resolved by mediation.

4.16 Section 66 of the Ordinance is rarely invoked in court proceedings, possibly due to lengthy and costly litigation process, and the risk of having to pay the defendant's costs. To PCPD's knowledge, there is no award ever made by the Court on damages suffered by a data subject as a result of infringement of personal data privacy. There has been international criticism that the Ordinance does not provide a genuine remedy to the aggrieved data subjects. Proposal No. 6 will provide an aggrieved data subjects an alternative choice of seeking remedy in a simpler, quicker and more effective way.

4.17 Proposal No. 5 is not a direct solution and cannot replace Proposal No. 6. Due to resources constraint, not all aggrieved party will be granted legal assistance. According to the model of the Equal Opportunities Commission ("EOC") quoted in the Consultation Document, the relevant legislation empowers the EOC to accede to a request for legal assistance only if:-

(a) the case raises a question of principle; or

(b) it is unreasonable to expect the applicant for legal assistance to deal with the case unaided, having regard to the complexity of the case or the applicant's position in relation to the respondent or another person involved or any other matter.

4.18 It should be noted that the opponent that an aggrieved data subject may face is usually an organizational data user who has ample resources (in terms of both manpower and monetary) to contest any civil action taken by the data subject. The PCPD considers that in order to provide adequate assistance to the aggrieved data subject, both proposals should be taken on board. In addition, these two proposals will serve direct deterrent effect on data users against infringement of the Ordinance.

Other comments

4.19 In conjunction with the power to be given under Proposal Nos. 5 and 6, the PCPD proposes 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 power under the Ordinance for the PCPD to carry out mediation of a complaint. Through the mediation process, the parties to a complaint may, with the PCPD acting as a mediator, agree to settle the complaint in an amicable manner. If the mediation is not successful, the PCPD may consider granting an award or providing legal assistance to the aggrieved data subject to institute civil action. The proposal may bring to the quick settlement of a complaint which is conducive to privacy protection and is in general accord with the current judicial approach of mediating prospective litigations.

Offences and Sanctions

Proposal No. 7 : Making Contravention of a DPP an offence

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

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

5.1 Proposal No. 7 to make contravention of a DPP an offence was not made by the PCPD. Proposal No. 8 to create a new offence of unauthorized obtaining, disclosure and sale of personal data was originally made by the PCPD[20] and modified by the Administration. Proposal No. 10 to impose penalty on serious contravention of DPPs was originally made by the PCPD[21].

5.2 At present, contravention of a DPP *per se* is not an offence. Instead, certain acts or practices have been singled out as offences under the current legislation. Examples are non-compliance with a data access or correction request (sections 19 and 23), failure to erase personal data no longer required for the purpose of their use (section 26), carrying out matching procedures other than in accordance with any conditions specified by the Commissioner (section 30), and direct marketing made by a data user to an individual who has previously requested the data user not to so use his personal data (section 34).

5.3 Making contravention of a DPP *per se* an offence will no doubt impact on civil liberty given the imminent risk of criminal prosecution. Strong grounds are needed for such a legislative proposal. Factors that are relevant for consideration will include:

(a) whether the contravening acts or practices in question are so serious that they need to be controlled by imposing criminal sanction; and

(b) whether the element of culpable intent is present.

---

[20] See PCPD's Proposal No. 41 at p.119 in the Annex to the Information Paper.

[21] See PCPD's Proposal No. 52 at p.139 in the Annex to the Information Paper.

5.4 A selective approach is preferred. It is also recognized under international jurisprudence that effective means of ensuring the proper behaviour and attitude towards protection of personal data privacy is by regulation rather than criminal sanction.

5.5 To deter contravention of a serious nature, the PCPD supports the approach to introduce a monetary penalty for serious contravention of the DPPs, modeling on the approach recently adopted by the UK Data Protection Act.[22] It aims at dealing with breaches of which the risk of their causing substantial damage or distress is known or ought to have been known to the data users. It sanctions against data users who wilfully disregard or are grossly negligent in complying with the requirements of the DPPs.

5.6 In line with the selective approach mentioned above, the PCPD supports the introduction of a new offence modeling on section 55 of the UK Data Protection Act 1998 in order to deter intentional or wilful acts that seriously intrude into an individual's personal data privacy, e.g. downloading or disseminating of personal data leaked into the Internet. The objective is not to penalize leakage or unintentional or accidental dissemination of personal data by a person, but to protect data subjects whose personal data were leaked and to deter irresponsible acts of obtaining or disclosure of such leaked data without the consent of the data users. It is also intended to close the loophole that "theft" of personal data is not an offence at present. For example, if a staff of a telecommunications company copies customers' personal data from the employer's records for the purpose of selling them to debt collection agents or third parties for profits, the staff concerned will not be criminally liable for theft of property.

5.7 The PCPD disagrees with the view that the proposal may interfere with the normal and innocuous browsing activities of web-users. There should not be a concern that innocent individuals may be caught by the new offence because, under the proposal, the person downloading personal data from the Internet may have a defence if he had the

[22] Section 144 of the UK Criminal Justice and Immigration Act 2008 amends the UK Data Protection Act by inserting under section 55A the power of UK Information Commissioner to impose monetary penalty. A full version of section 144 of the Criminal Justice and Immigration Act 2008 can be found at (http://www.opsi.gov.uk/acts/acts2008/ukpga_20080004_en_16).

reasonable belief that he had lawful right to obtain the personal data or that the data user would have consented to the obtaining. Only those who act *"knowingly or recklessly"* will be affected by the offence. It should also be noted that the proposed new offence should not prevent any person from invoking the exemptions under Part VIII of the Ordinance. In particular, section 52 of the Ordinance provides for an exemption from the provisions of the DPPs where personal data are held by an individual and concerned only with the management of his personal, family or household affairs, or so held only for recreational purposes.

5.8 As additional safeguard for journalistic activities, a separate defence on journalistic activities may be introduced for the new offence modeled on the amendment made to section 55(2) of the UK Data Protection Act under section 78[23] of the Criminal Justice and Immigration Act.

5.9 The PCPD does not prefer the proposed confinement of the new offence only to "*disclosure of personal data so obtained for (i) profits or (ii) malicious purposes"* as it will largely limit the scope of protection. It will hardly cover the loophole of the existing legal framework unveiled in the recent acquittal of a Taxation Officer of the Inland Revenue Department (ESCC3331/07), who was charged with one count of misconduct in public office, contrary to Common Law, because the prosecution failed to prove the reasons for his collection of taxpayers' personal data and the intended purpose of use. In that case, the Taxation Officer recorded the particulars (names, identity card numbers, business registration numbers, addresses and telephone numbers) of 13,400 taxpayers for his future personal use. There was no evidence to prove that the collection of the personal data had brought the Taxation Officer any financial gain. Such act, though serious in nature will not be caught under the existing proposal which is restricted to obtaining the data for "profits" or "malicious purpose".

5.10 In conclusion, the PCPD does not support any proposal to make contravention of a DPP *per se* an offence. For serious contravention, a

---

[23] It is a defence for any person who acted for the special purposes, with a view to the publication by any person of any journalistic, literary or artistic material and in the reasonable belief that in the particular circumstances the obtaining, disclosing or processing was justified as being in the public interest.

monetary penalty may be imposed. It is only for those acts or practices which are so culpable that they should then be singled out as offences under the Ordinance.

Proposal No. 9 : Repeated Contravention of a DPP on Same Facts
Proposal No. 11 : Repeated Non-compliance with Enforcement Notice

5.11 Both proposals were originally made by the PCPD[24] to curb repeated contravention of the Ordinance.

5.12 Paragraphs 6.15 and 6.24 of the Consultation Document state that there does not appear to be a strong case to introduce the above offences as the PCPD has not come across any such case since the enactment of the Ordinance.

5.13 For Proposal No. 9, it is not uncommon for different complainants to complain against the same data user at different times on the same or similar facts. The series of data loss incidents are real example of repeated contraventions. As for Proposal No. 11, the restricted enforcement power under section 50 of the Ordinance could be the reason that the PCPD has not come across repeated contraventions of an enforcement notice. As proposal has been made to amend section 50 by granting wider discretionary power on the PCPD to issue enforcement notices (see Proposal No. 20), it is foreseeable that more enforcement notices will be issued if the proposal is adopted.

5.14 The imposition of heavier penalty on repeated offender is commonly found in other legislations.[25] The PCPD finds it justifiable to adopt a similar approach given the prevalence of direct marketing activities and that repeated offenders demonstrate their lack of remorsefulness for which higher penalty level is called for to prevent repeated infringement of personal data privacy.

---

[24] See PCPD's Proposal Nos. 39 and 40 at p.115 and 117 in the Annex to the Information Paper.

[25] For instance, section 39(1) of the Unsolicited Electronic Messages Ordinance (Cap. 593) provides that a person who contravenes an enforcement notice served on him under section 38 commits an offence. Section 39(2) states that a person who commits an offence under section 39 is liable on a first conviction, to a fine at level 6 (i.e. 100,000) and on a second or subsequent conviction, to a fine of $500,000, and in the case of a continuing offence, to a further daily fine of $1,000 for each day during which the offence continues.

5.15 While statistics are not available, the PCPD believes that a proactive and forward-looking attitude should be adopted in order to enhance data privacy protection at this electronic age. The principle that is behind these Proposals is to be supported.

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

5.16 This proposal was originated from the PCPD[26] was made to increase the penalty level for misuse of personal data in direct marketing activities. The maximum penalty ($10,000 at present) under section 34 is hardly a deterrent. The relatively higher level of penalties imposed under the Unsolicited Electronic Messages Ordinance (Cap. 593) ("UEMO") which deals with unsolicited commercial electronic messages may be of some reference value.

5.17 The examples below show that the penalty level under the Ordinance at present is grossly insufficient:-

> ***Case 1***
>
> *In January 2007, a telecommunications company was convicted of breaching section 34(1)(ii) of the Ordinance. The case was heard at Kwun Tong Magistrates' Courts where four summonses were laid against the company for contravening section 34(1)(ii) of the Ordinance, which requires data users to cease to further contact the individual if he chooses to opt-out.*
>
> *The company began contacting the complainant by phone to promote its IDD services in July 2005. The complainant asked the company several times to stop calling him for direct marketing purposes. Nonetheless, the company continued to call him on a number of occasions for direct marketing purposes despite his opt-out requests. In February 2006, the complainant*

[26] See PCPD's Proposal No. 29 at p.85 in the Annex to the Information Paper.

lodged a complaint with the PCPD.

In July 2006, the PCPD issued a written warning to the company requiring it to cease making direct marketing calls to the complainant. In August 2006, the complainant received at least four marketing calls from the company. The PCPD concluded that the reoccurrence of the incidents was contrary to section 34(1)(ii) of the Ordinance and therefore referred the case to the Police for prosecution.

The company pleaded guilty to all summonses. The magistrate imposed a fine of $5,000 for the first summons, and $3,000 each for the 2nd to 4th summonses, making a total fine of $14,000 for the four summonses.

Case 2

In August 2007, a credit card company was convicted of two offences involving direct marketing activities in the Eastern Magistrates' Court.

The complainant was formerly a credit card holder of the company but cancelled the card account sometime in 2002/2003. Thereafter, the company sent several direct marketing mails to the complainant. In October 2005, the complainant made an opt-out request to the company by telephone. However, the complainant continued to receive direct marketing mail from the company. The complainant lodged a complaint to the PCPD in January 2006.

Having learned that the complainant had made a complaint to the PCPD, the company sent a letter of apology to him. The company also agreed to process the complainant's opt-out request by removing his data from their mailing list. Notwithstanding these actions taken, the complainant still received marketing mails from the

company on 15 January and 3 February 2007 respectively.

Consequently, the company was summonsed for two offences for breach of section 34(1)(ii) of the Ordinance. The company pleaded guilty to both summonses and the magistrate imposed a fine of $3,500 for each summon, which made a total fine of $7,000.

5.18 The Magistrate in Case 1, Mr. Chan Yan-tong, remarked that such direct marketing calls were "disgusting and annoying". He also commented that the maximum penalty of HK$10,000 hardly acted as a deterrent for large organizations.

5.19 The PCPD therefore supports that the penalty level for misuse of personal data in direct marketing be raised to a level of sufficient deterrent effect.

Penalty Level

5.20 Section 64 of the Ordinance sets out different levels of sanctions to be imposed in proportion to the gravity of the offence. The lowest level of sanction is found in section 64(5) and (10) at a maximum fine at level 3 ($10,000) for contravention of a condition of the PCPD's consent to a matching procedure and contravention of a requirement under the Ordinance. A higher level of punishment is imposed at a maximum fine at level 3 ($10,000) and imprisonment for 6 months for offences committed under section 64(1), (2), (3), (4), (6) and (9) which primarily relate to supply of false or misleading information in a data user return, data access or correction request, any matching procedure request, breach of duty of secrecy by the PCPD and his staff, and unlawful obstruction or non compliance with the lawful requirement of the PCPD. The highest level of punishment is found in section 64(7) for contravention of an enforcement notice, under which the offender is liable on conviction to a maximum fine at level 5 ($50,000) and imprisonment for 2 years and, in the case of a continuing offence, to a daily penalty of $1,000.

5.21 The PCPD recognizes that penalty levels should commensurate with the

adverse consequence of a breach, the harm caused to an individual, the relative importance of the rights to be protected and the seriousness of the offence as compared with other crimes. For existing offences, the PCPD proposes to increase the penalty level. As for proposed new offences, the PCPD proposes to keep pace with the penalty levels of similar offences in other legislation, thereby closing the gap of disparity of treatment. To facilitate the Administration to review the penalty level, the PCPD has prepared a ranking table at Table 1 below based on our assessment of the gravity of different offences.

5.22 The PCPD does not have strong views on whether a custodial sentence should be imposed on the proposed new offence of knowingly or recklessly obtaining personal data without consent. The UK Government is proposing to increase the penalty level to imprisonment for 2 years on indictment, and up to 12 months on summary conviction.[27] This is in addition to the fines not exceeding the statutory maximum (currently at £5,000) on summary conviction or unlimited fines on indictment. As for contravention of section 34(1)(ii), the penalty level of offences in the UEMO may be of reference value. The PCPD proposes that the levels of fines to be imposed on these two offences should be higher. In analyzing the assessment, readers should note that offence attracting custodial sentence is generally regarded as more severe punishment than a fine. The table below sets out how the PCPD ranks the offences.

Table 1 - Ranking of Existing and Proposed Offences (For ranking of penalty level purpose)

Section/ Proposal No.	Offence Details	Ranking (1 being the lowest, 6 being the highest)
Proposal No. 11	• Second or subsequent conviction for contravention of an Enforcement Notice	6

[27] See UK Ministry of Justice's Consultation Paper on "The Knowing or Reckless Misuse of Personal Data – Introducing custodial sentences" published on 15 October 2009, available at http://www.justice.gov.uk/consultations/docs/data-misuse-increased-penalties.pdf. The consultation will end on 7 January 2010.

Proposal No. 9	• Repeated contraventions of the Ordinance on the same facts where the first infringement has resulted in the issuance of an Enforcement Notice.	5
Existing 64(7)	• Contravention of an Enforcement Notice	4
Existing 64(1)	• Supply of false or misleading information in a material particular and in purported compliance of the notice under sections 14(4) (Data user return), section 14(8) (Prescribed information in the data user return) and section 15(3) & (4) (Prescribed information for the register or any change thereof)	3
Existing 64(2)	• Supply of information in a data access request or data correction request which is false or misleading in a material particular	3
Existing 64(3)	• Supply of false or misleading information in a material particular in a notice under section 15(6) (Cease to be data user)	3
Existing 64(4)	• Supply of false or misleading information in a material particular for the purpose of matching procedure	3
Existing 64(6)	• Contravention of section 44(3) (non-disclosure of identity under news immunity) or section 46(1) (duty to maintain secrecy)	3
Existing 64(9)	• Obstruction of performance of function by the Commissioner or failure to comply with the lawful requirement of the Commissioner, making a false or misleading statement to the Commissioner.	3
Proposal No. 12	• Contravention of section 34(1)(ii) for direct marketing activities	2

Proposal No. 8	• Knowingly or recklessly obtaining personal data without consent from the data user and the disclosure or sale of the data so obtained to third parties.	2
Existing 64(5)	• Contravention of conditions under a notice under section 30(2) (matching procedure) or 32(1)(b)(i) (matching procedure)	1
Existing 64(10)	• Contravenes a requirement under the Ordinance (other than a DPP) without reasonable excuse [Relevant acts covered by the offence being brought under this section:- - Section 23 (Data access request and data correction request), section 26 (Erasure of personal data), section 14 (Data user return) & section 34(1)(i) (Provision of opt-out choice).]	1
Proposal No. 1	• Contravention against the new provision for dealing with "sensitive personal data".	1
Proposal No. 24	• Contravention against the requirement for destruction/return/use of personal data under the new "mergers, acquisition and transfer of business" exemption under Part VIII.	1

Rights of Data Subjects

Proposal No. 13 : Third Party to Give Prescribed Consent to Change of Use of Personal Data

6.1 This proposal was originated from the PCPD[28]. It aims to permit the parents or guardians of a vulnerable data subject to give consent on his/her behalf to the change of use of his/her personal data. It must be stressed that this proposal is designated to deal with specific cases where the use of an individual's personal data may need a change for his/her own benefit, but that individual lacks the capacity to give a voluntary and informed consent to such change of use under DPP3.

6.2 The PCPD's proposal seeks to allow a "relevant person" to give "prescribed consent" on behalf of that individual. The term "relevant person" under the existing Ordinance means (i) where the individual is a minor, a person who has parental responsibility for the minor; or (ii) where the individual is incapable of managing his own affairs, a person who has been appointed by a court to manage those affairs. The PCPD did not propose the widening of the class of persons to be "relevant person".

6.3 A minor's capacity to give prescribed consent under DPP3 has drawn more attention from the general public. To begin with, it is important to note that specific right of privacy for children is recognized in Article 16 of the United Nations *Convention on the Rights of the Child 1989* which is applicable to Hong Kong:-

> *"1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.*
>
> *2. The child has the right to protection of the law against such interference or attacks."*

6.4 A number of approaches may be considered in the assessment of the

---

[28] See PCPD's Proposal No. 5 at p.17 in the Annex to the Information Paper.

capacity of individuals under the age of 18, such as:-

(a) determination of a young person's capacity to understand on a case-by-case basis;

(b) by fixing an age over which the young person shall be taken as having the capacity;

(c) the combination of (a) and (b) above: i.e. by setting an age over which the minor shall be taken as having capacity, and setting another age under which the minor shall be taken as not having capacity. Capacity of minors between these two ages would require individual assessment.

(d) Setting certain ages of legal capacity for the particular context of the decision, e.g. by setting a particular maturity age in relation to certain sensitive issues such as information relating to pregnancy;

(e) according to specific group of young people, e.g. by deeming young people who are married, parents themselves or living independently to have legal capacity.

6.5 The person making the assessment of the minor's capacity may not be suitably qualified to make the assessment. While setting a minimum age should overcome the difficulties in making individual assessment, the oversimplified solution is arbitrary and may cause injustice. The PCPD's research on the decision-making capacity supports the approach of making individual assessment in the interest of fairness.

6.6 Individual assessment generally accords with the common law position of "Gillick competency" test introduced in the UK landmark decision of Gillick v West Norkfolk and Wisbech Area Health Authority and Another [1986] 1AC112. The case sheds light on the proper test to apply when assessing an individual's competency. It concerns the prescription of contraception by a medical doctor to a minor at her request. The test sets out the criteria for doctors and other health professionals to apply in ascertaining, where there is a conflict of interest between a child or young person and his/her parents, whether

medical advice or treatment can be given without the consent or knowledge of the parents. A child or young person who is judged after consideration of these criteria as having the capacity to consent is often referred to as being "Gillick competent". The House of Lords (by a majority of 3 to 2) held that parental consent was not required, and the following guidelines were established when a child or young person sought confidential medical advice:

(a) If a doctor was of the view that the procedure could be said to be in a child's best interests; and
(b) If that doctor could not persuade the child to tell his/her parents; then
(c) Provided that the child was able to understand the nature and consequences of the medical procedure,

the child was competent to consent without the knowledge and consent of his/her parents.[29]

6.7 The guidelines laid down in the case have been in use by professionals dealing with children and young people in other areas where consent is necessary.

6.8 The approaches adopted by overseas jurisdictions are set out in the table below:-

Jurisdiction	**Approach**
Privacy Act 1985 (Canada)	➢ An authorized person may exercise or perform on behalf of a minor rights or actions.
Data Protection Act 1998 (UK)	➢ An individual under the age of 16 may exercise any right conferred by the *Act* where he has a general understanding of what it means to exercise that right. Such understanding is presumed where the individual is 12 years old or above.[30]

[29] See p.91 of "Children's Databases – Safety and Privacy", a report for the UK Information Commissioner issued in November 2006.

[30] See section 66(2) of *Data Protection Act 1998 (UK)* and *"Data Protection Act 1998 Legal Guidance (2001)"* issued by the UK Information Commissioner.

Privacy Act 1993 (New Zealand)	➢ An organisation is entitled to refuse to disclose information requested by an individual under the age of 16 if the disclosure would be contrary to the individual's interest.[31]
Personal Health Information Protection Act 2004 (Ontario)	➢ A person aged 16 or above can consent to collection, use or disclosure of his/her personal information. ➢ A parent, children's aid society or other person with parental responsibility may provide consent on behalf of an individual who is under 16 *but not if* information relates to : (i) medical treatment about which the individual has made his or her own decision; or (ii) child and family services counseling in which the individual has participated on his/her own. • *However, if* the individual is considered to be capable of consenting on his/her own, then the individual's decision prevails over the conflicting decision of the parents or other substitute decision-maker.[32]
European Union Article 29 Data Protection Working Party Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools)	➢ As a human, the child has a right to privacy. The core principle is that of the best interest of the child. ➢ If the processing of a child's data began with the consent of their legal representative, the child concerned may, on attaining majority, revoke the consent. But if he wishes the processing to continue, it seems that the data subject may need to give explicit consent wherever this is required. ➢ The principle of the best interest can have a double role. Situations may arise where the best interest of the child and his/her right to privacy appear to compete. In such cases, data protection rights may have to yield to the principle of best interest. This is particular the case for medical data. For example, a youth welfare service may require relevant

[31] See section 29(1)(d) of *Privacy Act 1993 (New Zealand)*.
[32] See section 23(2) and (3) of the *Health Information Protection Act 2004 (Ontario)*.

	information in case of child neglect or abuse. Similarly, a teacher may disclose a child's personal data to a social worker in order to protect the child, either physically or psychologically. ➢ Where consent is concerned, the solution can progress from mere consultation of the child, to a parallel consent of the child and the legal representative, and even to the sole consent of the child if he or she is already mature. ➢ The first level of the right to participate is the right to be consulted. ➢ The data protection needs of children must take into account two important aspects. Firstly, the varying levels of maturity which determine when children can start dealing with their own data. Secondly, the extent to which representatives have the right to represent minors in cases where the disclosure of personal data would prejudice the best interests of the child.
Privacy Act 1988 (Australia) *Australian Law Reform Commission Report issued on 11 August 2008*	➢ Currently, there is no provision for a child to give "consent". ➢ In relation to the question of capacity, the research conducted shows that an individual's capacity to make a decision cannot be determined by age alone.[33] ➢ It is also recognized that an individual approach to assess the capacity of a child or young person by way of the Gillick's test is the fairest and most appropriate way.[34] ➢ It is nevertheless acknowledged that the policy approach of setting a minimum age may have the advantage of clarifying the operation of the law and simplifying the process of determining capacity by data users.[35] ➢ Recommended model: • Where it is reasonable and practicable to make an assessment about the capacity of

[33] Paragraph 68.37 of the ALRC Report.
[34] Paragraph 68.102 of the ALRC Report.
[35] Paragraph 68.57 of the ALRC Report.

	an individual under the age of 18 to give consent, make request or exercise a right of access under the Act, an assessment about the individual's capacity should be undertaken. • Where an assessment of capacity is not reasonable or practicable, then an individual, (a) aged 15 or over is presumed to be capable of giving consent, making a request or exercising a right of access; and (b) under the age of 15 is presumed to be incapable of giving consent, making a request or exercising a right of access. • Where an individual under the age of 18 is assessed or presumed to not have capacity under the *Act*, any consent, request or exercise of a right in relation to that individual must be provided or made by a person with parental responsibility for the individual.

6.9 While there is no uniform approach taken, the generally recognized approach is to assess the young person concerned on individual cases.

6.10 In deciding what is in the "best interest" to serve, the duty lies upon the person who gives such consent on behalf of the minor to show that it serves a clear benefit to the minor having regard to the extent of intrusion into personal data privacy of the minor and the benefits or privileges to be derived. For example, deciding the proper course of medical treatment to be received may be regarded as safeguarding the vital interest of the minor. Reasonableness and proportionality are the benchmarks to measure.

6.11 It should be borne in mind that this proposal is applicable only when there is a change of the use of the minor's personal data and does not apply in the ordinary course of personal data handling.

Proposal No. 14 : Parents' Right to Access Personal Data of Minors

6.12 The proposal was originally made by the PCPD[36] at the request of the social welfare sector to permit a data user, in exceptional circumstances, to refuse to comply with data access requests made by the parents on behalf of their children in order to protect the interest of the children.

6.13 Data users should be able in appropriate cases to refuse to comply with a data access request where disclosure would be contrary to the interest of the minors. The proposal models on the New Zealand approach laid down in section 29(1)(d) of the Privacy Act 1993 which provides a ground for refusal to disclose personal information of an individual under the age of 16 if the disclosure would be contrary to the individual's interest.

6.14 Paragraph 8 in Annex 1 of the Consultation Document lists the exceptional instances that a data user may refuse to comply with the data access request. They are:-

(a) where the parent may abuse the data access mechanism to obtain the personal data of the child for the parent's own purpose rather than making it "on behalf of" the child. For instance, an estranged parent may make a data access request to the school or social welfare organizations for his/her child's location data to trace the whereabouts of the child or the other parent of the child;

(b) where a parent is suspected to have committed child abuse on his/her child; and

(c) where the child has expressed to the data user (at the time when providing his/her personal data to the data user) his/her disagreement to the disclosure of the data to his/her parents.

6.15 It should be noted that the exercise of this proposed ground of refusal is only in exceptional and unusual situations and in most of the other situations, data users may not have justifications to refuse to provide the

[36] See PCPD's Proposal No. 20 at p.57 in the Annex to the Information Paper.

minor's personal data to the parents. Data users may run the risk of breaching the provisions of the Ordinance by unjustified reliance on this proposed ground of refusal. An aggrieved parent may lodge a complaint with the PCPD in such instances.

6.16 For the situation in 6.14(a) above, the PCPD has come across specific cases which show justification to cater for the situation. An example is given below:

> *In 2003, the ex-husband of the complainant lodged with a data user several data access requests as the relevant person of his daughter, who no longer lived with him, for information relating to the school in which the daughter was studying. The father claimed that he had no knowledge as to the daughter's whereabouts after divorce. Under DPP3, except with the prescribed consent of the data subject, the data user may not disclose personal data for such purpose other than a purpose which is the same as or directly related to the original purpose at the time of collection. In relation to one of the data access requests, the data user disclosed the personal data of the daughter with which the father managed to locate the daughter and caused nuisance to the complainant and the daughter. After investigation, the PCPD warned the data user that such disclosure of the daughter's personal data was not directly related to the original purpose at the time of collection of the daughter's personal data.*

6.17 As for the situation in 6.14(b) above, where a parent is suspected to have committed child abuse, disclosure of the minor's personal data may endanger the well-being of the child.

6.18 The reason for the inclusion of the situation in 6.14(c) is that some data users are concerned about the possibility of inhibiting the minors from seeking counseling or other professional services if their personal data are disclosed to their parents.

6.19 The proposal has drawn attention from the public. There has been concern that the proposal may deprive the parents the right to access the personal data of their children such as school records. The PCPD has

stressed that the proposal only seeks to deal with specific situations as outlined in the proposal and it has never been intended to deny the parents' right to access personal data relating to the minors' education and development. In the case of school records, one of the original purposes of the school in collecting the students' personal data (such as performance in school) is for education and development of the students. The release by the school to the parents such personal data of the students without the students' consent does not infringe the Ordinance.

6.20 Another concern raised is that the requirement of *"best interest of the minors"* should be clearly defined. It must however be noted that giving the phrase *"best interest"* a specific definition may be undesirable. In many instances, the case should be decided on its own facts after taking all the circumstances into consideration so as to assess the *"best interest of the minors"*. The PCPD does not object the approach suggested by the Administration to consider the appropriateness of specifying some factors to enable the data users to assess whether there are reasonable grounds in exercising the proposed right of refusal in dealing with such data access requests. It should however be borne in mind that giving the term too restrictive a meaning may defeat its original purpose.

Proposal No. 27 : Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship

6.21 This proposal did not originate from the PCPD. The Administration puts forward this proposal to provide for an exemption to allow data users to transfer personal data of a minor that are relevant to parental care and guardianship to the parents or guardian of the minor, so that the latter can fulfil their responsibility to exercise proper care and guardianship of their children under the age of 18. The PCPD appreciates the rationale behind the proposal which will facilitate parents to provide care and guidance to their children in time. In order that the transfer is justifiable, consideration should be given to the type of the exempted personal data, the degree of disclosure and the relevant circumstances at the material time. Also, a mechanism must be built in to guard against misuse. Moreover, it is imperative for Administration to consider allowing minors who attain certain age to make their own

decisions in relation to the disclosure of the personal data.

6.22 Apart from the option of providing specific exemption in the Ordinance, the Administration may consider whether the best solution to tackle the situation as identified in the proposal be by way of other child protection laws.

6.23 The PCPD has made enquires with overseas privacy regulators whether similar exemption is provided under their privacy legislation for the transfer of minors' personal data to the parents that are relevant to parental care and guardianship. The replies reveal that there is no equivalent or similar exemption under the overseas privacy legislation.

6.24 Take the situation in the UK for example, under section 29 of the Data Protection Act, an exemption is provided to allow disclosure of personal data if that will aid the prevention or detection of crime or the apprehension or prosecution of offenders. It covers situation where the police is of the view that the disclosure of the personal data about a minor to their parents might prevent a crime. However, in situation where there is far from "concrete evidence" of a crime (as mentioned in paragraph 65 Annex 1 of the Consultation Document), it will be covered by a wide range of local legislation in the UK which relates to ***child protection***. The relevant legislation lays emphasis on the experienced professionals empowered to make decisions which the child is unable to do so for themselves in circumstances where the child's overall well-being may be compromised. These decisions will at times include decisions to disclose personal data about the child. Unlike the police, the childcare professionals, social workers and teachers do not have to have "concrete evidence" before they may act. They simply have to show that in their professional opinion that it is in the child's best interests to disclose the relevant personal data.

Enhancing the Effectiveness of Ordinance

7.1 The PCPD supports all proposals raised in the Consultation Document that will enhance the effectiveness of the Ordinance.

Proposal No. 20 : Circumstances for Issue of an Enforcement Notice

7.2 This proposal was originally made by the PCPD[37]. It aims to relax the current overly restrictive criteria for issuing an enforcement notice by the PCPD. The option proposed by the Administration in paragraph 39 of Annex 1 of the Consultation Document, if adopted, will to a certain extent allow PCPD to exercise the right of issuing an enforcement notice in a more effective manner, thereby enhancing the protection to the individuals affected.

7.3 In addition to the option, the PCPD considers that its discretion will be more effectively exercised if a further option is provided to *consider other matters as the PCPD may think fit* when deciding whether to issue an enforcement notice. This option will enable the PCPD to consider also other relevant circumstances in the specific cases. In deciding whether to issue an enforcement notice, the PCPD wishes to be able to consider, amongst other things, the following:-

(a) whether it is in the interest of the public;

(b) the gravity of the contravention, including the number of individuals affected and the type of personal data involved;

(c) whether or not the data user has in place any data protection policy concerning the contravening act or practice;

(d) whether or not the act in question is deliberate or accidental or an isolated incident;

(e) the conduct of the data user during the incident in question, after being notified of the subject matter of the complaint (whether by the complainant, the media, PCPD, other regulators or other

[37] See PCPD's Proposal No. 19 at p.54 in the Annex to the Information Paper.

sources), and during the course of the investigation (whether co-operative, whether providing misleading information, whether remorseful, etc.);

(f) whether the data user has remedied the contravention during the course of investigation, whether or not the data user has unreasonably delayed the remedial action;

(g) whether or not the data user has offered to compensate the complainant;

(h) whether there are previous complaints against the data user and taking into account the circumstances of those complaints;

(i) whether or not the data user has previously found to have been in contravention of the Ordinance, irrespective of the nature of the act or practice concerned in the previous contravention.

7.4 The PCPD believes that to introduce more flexibility under section 50 to serve an enforcement notice will enhance data privacy protection in that data users in contravention of the Ordinance will be directed under the enforcement notice to take specific steps to remedy the contravention and failure to do so is a criminal offence.

7.5 Below are some case examples which the PCPD's discretion to issue an enforcement notice was restricted by the current section 50.

Case 1

The complainants (a couple) instructed a company to prepare their wills and they discovered that the company had adopted the wife's will as a template to draft the will of another client and forwarded a softcopy of the draft will for that client's approval. In the margin of the draft will, there were boxes printed with information of the wife's will as well as personal data of the husband. It was caused by the "check change" feature of the word processing software having been enabled during the process.

The company took remedial actions by (i) convening a meeting with all staff discussing the incident, running through the workflow again and explaining the consequences of not following the procedures (ii) devising a new workflow checklist to make sure that draft will was in correct format which has to be signed by the staff concerned and countersigned by the superior of that staff; (iii) giving a warning to the staff concerned who released the complainants personal data; and (iv) making an apology to the complainants.

In view of the remedial actions taken by the company, the PCPD found no evidence of likelihood of repetition of the contravention. Hence no enforcement notice was issued despite the serious intrusion of the complainants' personal data privacy.

Case 2

A complainant alleged that a telecommunications company had a practice of re-activating its customers' lockout account by automatically resetting his or her password to a fixed number of 123456, thus exposing the customer's personal information contained in its electronic billing system to the risk of intrusion by unauthorized third parties. Subsequently, the telecommunications company took remedial measures on password resetting. In view of the remedial actions taken, the PCPD found no evidence of likelihood of repetition of the contravention. Hence no enforcement notice was issued.

Case 3

The complainant alleged that a company had collected a copy of her Hong Kong identity card prior to the granting of a job interview. Upon intervention by the PCPD, the

company confirmed that they had destroyed all HKID copies of job applicants previously obtained, and undertook that they would not collect the HKID copies of job applicants unless and until the individual had accepted an offer of employment. In light of the above remedial actions taken by the company, the PCPD had not served an enforcement notice since no evidence of likelihood of repetition of the contravention could be found.

Case 4

The complainant had a dispute with a travel agent over the amount to be charged on cancellation of an air flight booking. The complainant later discovered that the travel agent had, without his consent, used the personal data collected during the booking transaction for lodging a complaint against him to his employer thereby disclosing the details of the dispute. Upon investigation by the PCPD, the travel agent confirmed that (i) she would not use the complainant's personal data for any purpose other than air flight booking and related matters; (ii) the information collected during booking transaction had formed part of internal document retained by employer of the travel agent and she had not retained a copy of the complainant's personal data. In view of the aforesaid, the PCPD did not issue an enforcement notice as no evidence of likelihood of repetition of contravention was found.

Case 5

The complainant opened an account with a ticket company for purchasing cinema and concerts tickets online by credit card. During online registration, the complainant chose not to receive direct email newsletter but he still received 3 marketing emails from the company at his email address. Subsequently, the company took remedial actions by (i) removing complainant's email address from

the mailing list (ii) amending the opt-out statement; and (iii) conducting manual check of mailing list to ensure no inclusion of subscribers who had opted out. In view of the remedial actions taken, there was no evidence of likelihood of repetition of the contravention by the company. Thus, no enforcement notice could be served on the company by the PCPD.

Case 6

In this case, the complainant borrowed from a bank a property mortgage loan. She later indicated to the bank that she intended to sell her property at a price less than the outstanding mortgage loan owed to the bank. The bank offered her a loan covering the shortfall balance to be repayable by 24 equal monthly instalments. The bank however treated the mortgage loan account as an account in default and notified the Credit Reference Agency of the above as a scheme of arrangement. The complainant complained that she had never been in default of the mortgage loan and the shortfall loan. Upon investigation by the PCPD, the bank asked the Credit Reference Agency to delete the purported default data, which the CRA had acted accordingly. In view of the remedial action taken by the bank, the PCPD opined that the contravention was not likely to be repeated and therefore no enforcement notice was issued.

Case 7

The complainant ceased to be a customer of a telecommunications company. Later, he discovered that the telecommunications company debited his credit card for a service fee. As the complainant had never provided his credit card number to the company, he lodged a complaint with the PCPD. Investigation by the PCPD revealed that the telecommunications company had made a clerical mistake by wrongly debiting the complainant's

credit card account for a fee incurred by another customer. The telecommunications company stated that they had a policy in place requiring their staff to verify the accuracy of customers' personal data and in order to avoid recurrence of similar incident in future, they had advised their staff to double-check the credit card account number before transferring the same to the bank. In view of the remedial action taken by the company, the PCPD opined that the contravention was not likely to be repeated and therefore no enforcement notice was issued.

Case 8

The complainants complained that a company provided online service to their subscribers for retrieval of individuals' ownership of properties. The PCPD's investigation revealed that the personal data contained in the database of the company were purchased from the Land Registry and the company had used the data for a purpose outside the purpose of use as stipulated by the Land Registry. To remedy the situation, the company ceased providing the service to their customers. Given the remedial action taken by the company, the PCPD did not issue an enforcement notice since there was no likelihood of repetition of the contravention.

7.6 In each of the cases above, had the PCPD not been tied by the restrictions under section 50, it could have served enforcement notices on the parties complained against directing them to cease doing any act or engaging in any practice which caused the infringement. It will have a deterrence effect on the parties concerned since any breach of the directions of an enforcement notice is a criminal offence.

7.7 Added to those cases is the situation that the PCPD is not able to issue an enforcement notice directing a data user to destroy personal data collected by unfair means where the contravening act of collection had ceased and there is no evidence suggesting that the contravention will

continue or be repeated[38]. This is undesirable as the protection of personal data privacy has been compromised by the overly restrictive criteria for issuing an enforcement notice.

7.8 There should not be concerns that the additional option will confer unfettered discretion on the PCPD. It is because pursuant to the current provision of the Ordinance[39], a data user who has been served with an enforcement notice may lodge an appeal to the Administrative Appeals Board (AAB) against the PCPD's decision. Hence, if PCPD's discretion is not reasonably exercised, his decision will not stand before the AAB.

7.9 The PCPD therefore urges the Administration to consider adding *"such other matters as the Commissioner may think fit to consider"* as paragraph (d) to the option raised in paragraph 39 of Annex 1 of the Consultation Document.

Proposal No. 21 : Clarifying Power to Direct Remedial Steps in an Enforcement Notice

7.10 This proposal originated from the PCPD[40] was made for the purpose of stating explicitly the PCPD's power to direct the relevant data user in an enforcement notice to desist from doing an act or engaging in practice. This will clear up the grey area currently found in the Ordinance.

Proposal No. 22 : Removing the Time Limit to Discontinue an Investigation

7.11 This was a proposal originated from the PCPD[41] to remove the time limit imposed under section 39(3) of the Ordinance with regard to a decision to discontinue investigation. It is not effective use of the limited resources of the PCPD to continue to pursue unwarranted investigations. Hence, the PCPD supports this proposal to amend the Ordinance to make this clear.

---

38 See section 50(1) of the Ordinance
39 See section 50(7) of the Ordinance.
40 See PCPD's Proposal No. 19 at p.54 in the Annex to the Information Paper.
41 See PCPD's Proposal No. 13 at p.41 in the Annex to the Information Paper.

Proposal No. 23 : Additional Grounds for Refusing to Investigate

7.12 This proposal was originally made by the PCPD[42] to add the following grounds under section 39(2) of the Ordinance for refusal to carry out or continue an investigation initiated by a complaint:-

(a) where the primary cause of the complaint is not related to personal data privacy;

(b) the complaint relates to any action which the complainant has a remedy in any court or tribunal or is currently or soon to be under investigation by another regulatory body, unless the PCPD is satisfied that in the particular circumstances it is not reasonable to expect the complainant to resort or to have resorted to that right or remedy; or

(c) where the act or practice specified in the complaint relates to personal data or documents containing personal data which have been or will likely be or intended to be used at any stage in any legal proceedings or inquiry before any magistrate or in any court, tribunal, board or regulatory or law enforcement agencies.

7.13 As for the ground (a) *"where the primary cause of the complaint is not related to personal data privacy"*, a comprehensive study of the following complaint cases received by the PCPD will help to clarify the reasons why such a proposal was made.

Case 1

The daughter of the complainant posted a notice with the headline "The present chairman xxx arrogates all powers to himself" in the public area of the building.

In response to the notice, the chairman of the Incorporated Owners ("IO") xxx issued a memo, which contained the name of the complainant. In this connection, the complainant complained that the

[42] See PCPD's Proposal No. 12 at p.37 in the Annex to the Information Paper.

chairman of the IO had disclosed his personal data, and the IO "criticized owners with big-character poster of the Cultural Revolution".

The PCPD opined that from the nature of the incident (scolding and libel), the complaint was not related to personal data privacy.

Case 2

The complainant sent a letter to the owners of his building with respect to the re-election of the management committee of the building. The name and address of the complainant were stated in the letter.

In response to the letter, the Incorporated Owners ("IO") of the building issued a memo, which contained information of the complainant, such as name. In this connection, the complainant complained that the IO had disclosed his personal data.

The PCPD opined that the complaint mainly involved the expression of opinions to owners on the re-election of the management committee by the complainant and the IO. The complainant had disclosed his identity to the owners at the beginning. The cause of the complaint was not related to privacy.

Case 3

The complainant was a customer of a telecommunications company.

The telecommunications company intended to call the complainant to promote its service, but the call was picked up by the complainant's son, who accepted the service on behalf of the complainant. The complainant then complained that the telecommunications company used his

personal data to promote sales to his son.

The PCPD opined that the case mainly concerned the manner in which the telecommunications company's salesman promoted its service. It was not related to personal data privacy.

Case 4

The complainant was a customer of a telecommunications company and used credit card autopay to settle the bills.

Later, the complainant stopped using the credit card autopay service, but the company continued to use his credit card account to settle the bills. The complainant lodged a complaint with the PCPD.

The PCPD opined that the case mainly involved the settlement of bills between the service provider and the customer. It was not related to privacy.

Case 5

The complainant was an online game customer of an electronic game manufacturer.

The complainant was rejected to log in the game because he had wrongly registered as a minor.

After amending the date of birth, the complainant still could not log in. In this connection, the complainant complained that the manufacturer had retained and used the data which were not updated.

Enquiry with the manufacturer revealed that it had recorded the correct date of birth of the complainant. The PCPD took the view that the incident was caused by the setting of system of the manufacturer. It was not

related to personal data privacy.

7.14 It is self-evident from the above cases that the primary causes of the complaints are not related to personal data privacy.

7.15 There are also complaints caused by personal feud. In this connection, the AAB in AAB Appeal No.24 of 2001 stated as follows:-

> *"The Board wish to make it known that we deprecate any attempt by persons to use the Board as a forum for the pursuit of personal vendetta or to vent their anger. The Ordinance must be interpreted and applied sensibly, reasonably and practicably so that it is not used as a tool of oppression or revenge."*

7.16 The PCPD agrees with the observation made by the AAB. Very often, it is found that some complainants have utilized the complaint channel provided under the Ordinance for personal feud rather than being motivated by a genuine concern for protection of one's personal data privacy. The PCPD considers that the complaint channel under the Ordinance should not be used as a forum for the pursuit of personal dispute not related to personal data privacy.

7.17 The Administration has expressed reservations in respect of ground (b) "*if the complaint relates to an action for which the complainant has a remedy in any court or tribunal"* because it would deprive an aggrieved party of a redress alternative. The PCPD considers that in some cases, the PCPD may not be an appropriate forum for the aggrieved individual to seek redress, when compared with the sanction imposed under other laws or ordinances. For example, where a complaint involves a disgruntled employee seeking redress against the employer's termination of his employment, the PCPD finds it proper for the matter to be dealt with in the Labour Tribunal. In order to provide further safeguard to the aggrieved individual, the PCPD has considered and did make proposal for a saving clause. This is when in the particular circumstances it is not reasonable to expect the complainant to resort or to have resorted to the right or remedy in court or tribunal. In addition, the Ombudsman Ordinance also contains similar ground of refusal under

section 10(1)(e)(ii). This shows the Legislature's readiness to accept similar ground as valid refusal of a complaint.

7.18 With regard to ground (c), i.e. where personal data in question have been or will likely be or intended to be used at any stage in any legal proceedings or inquiry, the common example is where the complainant is engaging in a fishing expedition to obtain documents and data (through the lodging of a data access request) which he would otherwise only be entitled to under discovery procedures taken in legal proceedings. In a judicial review application[43], the Judge took the view that where the data subject had obtained or could have obtained copies of his personal data through legal proceedings, it would be meaningless and a waste of public funds for him to lodge a complaint with the PCPD on non-compliance with a data access request and for the PCPD to investigate the matter. In a judicial review application[44] made against the AAB's decision concerning compliance with a data access request lodged by the Appellant, the Court states in paragraph 34 of the judgment as follows:-

> *"It is not the purpose of the Ordinance to enable an individual to obtain a copy of every document upon which there is a reference to the individual. It is not the purpose of the Ordinance to supplement rights of discovery in legal proceedings, nor to add any wider action for discovery for the purpose of discovering the identity of a wrongdoer under the principles established in Norwich Pharmacal v Commissioners of Customs and Excise [1974] AC 133. That conclusion is entirely in accord with the decision of Deputy Judge Muttrie in Gotland Enterprises Ltd v Kwok Chi Yau [2007] HKLRD 236, at 231-2."*

7.19 The proposal to include three additional grounds of refusal aims to make good use of the PCPD's limited resources in handling complaints and

---

[43] 徐冠華 訴 個人資料私隱專員 [2004] 2 HKLRD 840
http://legalref.judiciary.gov.hk/lrs/common/search/search_result_detail_frame.jsp?DIS=39465&QS=%28%7Bhcal94%2F2003%7D%7C%7BHCAL000094%2F2003%7D+%25caseno%29&TP=JU

[44] Wu Kit Ping v Administrative Appeals Board, HCAL60/2007
http://legalref.judiciary.gov.hk/lrs/common/search/search_result_detail_frame.jsp?DIS=58956&QS=%28%7Bhcal60%2F2007%7D%7C%7BHCAL000060%2F2007%7D+%25caseno%29&TP=JU

should therefore be supported.

General comments

7.20 The critical success factor involved in the handling of complaints is that the PCPD should be permitted to utilize its limited resources by not having to investigate complaints where the general good of the public is not manifestly served. To achieve the goal of following up on every complaint in a painstaking manner is not the practice in overseas privacy or data protection authorities. PCPD simply has to be allowed to be selective in order to be effective having regard to the size of its organization.

Annex 2 to the Consultation Document - Proposals Not to be Pursued

8.1 Annex 2 to the Consultation Document contains 9 proposals that the Administration is not inclined to pursue after deliberating on the implications of the proposals. The PCPD's stance on each of the proposals is set out below.

Revamping Regulatory Regime of Direct Marketing

8.2 The Administration does not consider it appropriate to make further amendments to the regulatory regime of direct marketing under section 34 of the Ordinance.

8.3 The PCPD has, however, suggested the Administration to consider reviewing the regulatory regime with particular attention to the following aspects[45]:-

(a) whether to introduce an "opt-in" regime in place of the current "opt-out" regime;

(b) whether a territorial wide central "Do-not-call" register be established; and

(c) whether a data user shall disclose the source of the data upon the data subject's request.

8.4 The "opt-in" approach requires a data user to obtain the express consent of the data subject for the use of the latter's personal data. Such approach is in alignment with the "prescribed consent" under the use limitation principle expounded under DPP3. A territorial wide central "Do-not-call" register will serve as a clear notice and caveat to data users which intend to make telemarketing calls, not to use the personal data contained in the register for such purpose. As a further step to enhance protection to personal data, consideration may be given to require the data user, on request by a data subject, to disclose the source of his personal data collected by it. This suggestion was made to address the concerns raised by complainants on how organizations

[45] See PCPD's Information Paper, Issue No. 2 to the Annex at p.155-156.

obtained their personal data for making the unsolicited direct marketing communications to them.

8.5 The PCPD considers that conferring a right on the individuals to know the source of data will enhance transparency in how individuals' personal data is handled and promote the handling of personal data that accords with individuals' reasonable expectation over the use of their personal data. The Australian Law Reform Commission in its Report 108 – For Your Information: Australian Privacy Law and Practice[46] issued in August 2008 made a similar recommendation. In response to the recommendation, the Australian Government has recently accepted such recommendation and agreed that individuals should have the right to be so informed by the organization if they have not had a customer relationship with the organization[47].

8.6 Paragraph 5 of Annex 2 (p.72) of the Consultation Document states that 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 UEMO if the problem grows in future. In a recent paper[48] prepared by the Office of the Telecommunications Authority ("OFTA's Paper") to the Legislative Council Panel on Information Technology and Broadcasting, it stated that the use of personal data for direct telemarketing had already been regulated under the Ordinance and there was no clear need to contemplate further legislative measures for such calls. From this paper, it appears that no change will be made to UEMO to regulate person-to-person telemarketing activities. It is therefore necessary for the Administration to reconsider revamping the regulation of direct marketing activities involving the use of personal data in this opportune moment of reviewing the Ordinance.

8.7 OFTA's Paper contains the results of a public opinion survey and an industry survey commissioned by the Administration in respect of person-to-person telemarketing calls. It is noted from the summary of

---

46 Available at http://www.austlii.edu.au/au/other/alrc/publications/reports/108/26.html#Heading386

47 Recommendation 26-6 Australian Government First Stage Response to ALRC Privacy Report, p.59, available at http://www.pmc.gov.au/privacy/alrc.cfm

48 LC Paper No. CB(1)240/09-10(04), available at http://www.legco.gov.hk/yr09-10/english/panels/itb/papers/itb1109cb1-240-4-e.pdf

the public opinion survey that the respondents had not been asked about whether there was any need for the Government to expand the scope of the UEMO to cover person-to-person telemarketing calls involving the use of personal data. Nevertheless, the results of the survey reflected clearly the community concerns about direct marketing activities. It is revealed from the public opinion survey that:-

(a) Out of 967 respondents, 766 were always sure whether callers had their personal data or not. Among these 766 respondents, 55% reported that more than 40% person-to-person telemarketing calls received by them involved the use of their personal data.

(b) Out of the 806 respondents who had ever received person-to-person telemarketing calls in which callers had their personal data, only 35% of them had ever requested the callers not to call them again. Among those respondents who had ever made unsubscribe requests to callers, only 21% said that callers would honour their request. On the other hand, 30% said that callers would continue to call even though they had promised not to call again.

(c) About 81% of 967 respondents said that person-to-person telemarketing calls had caused inconvenience to them. When being asked to rate the level of inconvenience, over 30% considered such calls caused a lot of inconvenience to them, while almost half of them reported moderate inconvenience. The most often quoted inconveniences included wastage of time, being called when respondents were working or busy, and being called repeatedly.

(d) 57% of 1,157 respondents in the survey considered that the Government should regulate person-to-person marketing calls not involving the use of personal data. 42% of the total respondents supported regulation by legislation while 15% of the respondents supported to regulate such calls by a voluntary code of practice[49].

8.8 It is noted that there is no majority view to support regulation of

[49] Quoted from the OFTA's Paper.

person-to-person marketing calls not involving the use of personal data by legislation. However, it is totally different from the case of using personal data for direct marketing. The PCPD takes the view that the Administration should reconsider the need to tighten up the regulation of direct marketing activities involving the use of personal data under the Ordinance given the clear voice reflected in the community.

Internet Protocol Address as Personal Data

8.9 This proposal was originated from Yahoo's case[50] where heated debates had been raised on whether IP address should be viewed as "personal data". The Administration does not consider it appropriate to deem IP address *per se* as personal data under the Ordinance. The PCPD is open-minded as to the proposal but would like to set out the information below for consideration.

8.10 The existing three-limb definition of "personal data" gives general guiding principles on what constitutes "personal data" without singling out any particular kind of data to be so classified. The definition is of pretty straight forward application save for the concept of "indirect" identification and relevancy. In the past, the PCPD, in interpreting the meaning of what is "reasonably practicable" for the data user to ascertain the identity of the individual, has taken into account of other information that is readily obtainable by the data user.

8.11 The Yahoo's case raised concern on whether IP address falls within the definition of "personal data" as it can give useful hints for tracing the identity of the actual user of the computer. In the Yahoo's case, the PCPD took the view that an IP address *per se* does not meet the definition of "personal data". However, "personal data" can include an IP address when combined with, for example, identifying particulars of an individual.

8.12 The Yahoo's case went before the AAB[51]. The Appellant relied on *Cinepoly Records Co Ltd and others v Hong Kong Broadband Network*

---

[50] See PCPD's investigation report, available at http://www.pcpd.org.hk/english/publications/files/Yahoo_e.pdf

[51] AAB No. 16/2007, available at http://www.pcpd.org.hk/english/publications/files/Appeal_Yahoo.pdf

Ltd and others [2006] 1 HKLRD 255 to illustrate how an IP address might be used to track down the identity of a certain data subject. Having considered the evidence before it, the AAB dismissed the appeal and decided that on the facts of the case, the IP log-in information provided by Beijing Yahoo! even when coupled with other information disclosed, did not constitute "personal data" as defined under the Ordinance.

8.13 The public sentiment at the material times was very much concerned about the protection of IP address and questions were raised in the Legislative Council relating to disclosure of IP address without consent.

8.14 In view of the public concern, it is necessary to review whether IP address should be afforded the same protection of "personal data" under the Ordinance. The PCPD sets out below the pros and cons for deeming IP address as personal data.

Pros

- it gives certainty on its classification;

- it imposes obligations on persons, such as ISPs, webmail service providers and IT system administrators, etc to comply with the requirements of the Ordinance; and

- the disclosure of IP address to third parties, such as law enforcement bodies, would have to comply with DPP3 or otherwise the application of the relevant Part VIII exemption.

Cons

- IP address can be dynamic instead of static and there may be multiple users to a computer, e.g. in an office or cyber café environment. It may not be practicable to ascertain the identity of the user of the computer;

- IP address appears at the header of an email, affording it with the protection under Ordinance may have practical difficulties;

- onerous burden may be imposed on the ISPs and webmail service providers, particularly in situation when they have no intention to compile information about any individual when IP address is randomly allocated.

- If IP address is specifically defined as personal data, then email address, mobile phone number, car registration number, Autotoll tag number, Octopus card number etc. should logically be considered for inclusion on the ground that they are capable of "indirectly" identifying a particular individual by tracing. It would appear difficult to have an exhaustive list.

8.15 Added to the above complications is that new IP address standards (IPv6) have already been applied in some network segments (less than 1% of the WWW). Unlike the current IP addresses (IPv4), there is no "public" or "private" but universally unique IP address within IP v6 operations (while "static" and "dynamic" concepts would still apply). When compared to IPv4, an IPv6 address always represents a uniquely numbered computing device (usually operated by a person) in the WWW (even if such device is working behind a router or within a LAN). Unlike the situation in IPv4 (that identifying a device hosting a private IPv4 address could only be done by the LAN owner/operator), identifying an IPv6 host device may be possible on most of the data recipient's sides.

8.16 The question as to whether IP address alone shall be deemed as "personal data" is very controversial and the rights and interests of different classes in the society shall be fully and carefully considered before a decision should be made. PCPD is open-minded with regard to the proposal.

Territorial Scope of the Ordinance

8.17 This proposal was originated from PCPD[52] to exclude from the application of the Ordinance any act or practice involving personal data the collection, holding, processing and use of which occur wholly

[52] See PCPD's Proposal No. 6 at p.21 in the Annex to the Information Paper.

outside Hong Kong. The Administration is not inclined to pursue the proposal.

8.18 As it presently stands, the Ordinance is unclear as to whether it applies to cases where the act of collection, holding, processing and use of personal data take place wholly outside Hong Kong.

8.19 Section 39(1)(d) provides that where none of the conditions specified is fulfilled in respect of the act or practice complained of, the PCPD may refuse to carry out or continue with an investigation initiated by a complaint. One of the conditions specified under section 39(1)(d)(i)(B) is where *"the relevant data user was able to control, in or from Hong Kong, the collection, holding, processing or use of the personal data concerned"*.

8.20 Where personal data are "wholly collected, held, processed and used" by an organization or a person outside Hong Kong, the act or practice is likely to be subject to the applicable laws at the place that the act takes place or the practice is engaged in. By the operation of the territorial principle, certain territorial link with Hong Kong should exist in order for the Ordinance to apply.

8.21 It is however commented by the AAB in AAB No.16/2007[53] that section 39(1)(d) is not a provision dealing with extra-territorial application of the Ordinance and *"it does not provide the answer as to whether the Ordinance may have extra-territorial application"*. It was also decided that insofar as the person satisfies the definition of *"data user"* under the Ordinance exercising control over the personal data *"in or from Hong Kong"*, the Ordinance shall apply notwithstanding that none of the acts of collection, holding, processing or use of the personal data takes place in Hong Kong.

8.22 It would be unfair to the data user 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. It then follows that a data user will face the dilemma of either breaching the Ordinance if it authorizes disclosure of the personal data to a foreign law

[53] Available at http://www.pcpd.org.hk/english/publications/files/Appeal_Yahoo.pdf

enforcement authority or faces the legal consequence (sometimes involving criminal sanction) under the applicable foreign law if it fails to comply with the lawful order issued under that law. The PCPD will also face practical difficulty to gather evidence on such overseas act or practice.

8.23 To deal with the anomaly, the Ordinance should be amended to exclude from its application personal data the collection, holding, processing and use of which occur wholly outside Hong Kong.

8.24 In paragraphs 12 to 13 in Annex 2 of the Consultation Document, the Administration states that 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. The Administration is concerned that it might create a loophole in the proposed regime as a company in Hong Kong can arrange offshore collection of personal data by an agent and outsource the holding, processing and use of such data outside Hong Kong and it would make Hong Kong a data haven.

8.25 The PCPD does not see from the example given by the Administration that Hong Kong would become a data haven. According to the proposal, if any part of the data cycle of the personal data in question takes place in Hong Kong, the relevant data would still be protected under the Ordinance even if they are subsequently transferred outside Hong Kong. A Hong Kong company uses an offshore entity to collect personal data in Hong Kong, the company would still be caught by the proposed regime if the collection took place in Hong Kong. For those personal data that are collected, held, used and processed wholly outside Hong Kong, the PCPD does not see why they should be protected under the Hong Kong law. It should be noted that the LRC report was prepared 15 years ago. The situation should be reviewed in light of the economic development of the society during the last decade. Particularly, the PCPD is mindful of the proliferation of Hong Kong people establishing businesses outside Hong Kong, such as in the Mainland. For example, a person in Hong Kong owns a toy manufacturing business in the Mainland. The employees of the business are all employed in the Mainland and personal data of the

employees are collected, held processed and used wholly in the Mainland. The owner could not have expected that he had to comply with the Ordinance, being a Hong Kong law, in protecting the personal data of his employees in the Mainland. Nor could he have expected that the PCPD would have jurisdiction to deal with complaints made by his employees in the Mainland. It is also illogical to expect that, with so limited resources, the PCPD would be able to deal with complaints raised by complainants all over the world whose employers are in Hong Kong.

8.26 The PCPD therefore considers that it is highly desirable to consider the realistic proposition that the Ordinance should not apply to any act or practice involving personal data the collection, holding, processing and use of which occur wholly outside Hong Kong.

Public Interest Determination

8.27 This proposal was originally made by the PCPD[54] for the purpose of empowering the PCPD to make a public interest determination, with conditions, if any, imposed on a case-by-case basis upon application by the relevant data user. The Administration does not consider it appropriate to pursue such a proposal.

8.28 It is mentioned in paragraph 16 in Annex 2 of the Consultation Document that the proposal if instituted will undermine the certainty of personal data privacy protection afforded to data subjects. The PCPD does not agree with the view taken by the Administration. Many overseas jurisdictions have provisions in their data privacy legislations the public interest exemption.[55] Contrary to the Administration's view, the proposal, under which a data user who wishes to invoke public interest exemption shall apply to the PCPD for public interest determination, will provide for greater certainty by enabling a data user to release the relevant data in the public interest without contravening DPP3 where the circumstances require a timely disclosure.

---

[54] See PCPD's Proposal No. 33 at p.94 in the Annex to the Information Paper.

[55] See the relevant provisions of UK Data Protection Act, New Zealand Privacy Act and Australian Privacy Act as set out in paragraphs 14.2 to 14.5 of the Information Paper.

8.29 The Administration further states in paragraph 16 in Annex 2 of the Consultation Document that if there is justification to grant exemption on specific grounds, it is more appropriate to address them by way of specific public interest exemption. In PCPD's view, it is impracticable to provide an exhaustive list of public interest exemptions for or a public interest exemption that encompasses all appropriate situations. On the other hand, a general public interest exemption would provide for flexibility to accommodate all appropriate cases. The proposed public interest determination mechanism, which is operated on *ad hoc* basis upon application of the concerned data user, will enable the PCPD to determine whether there is justifiable overriding public interest that outweighs data privacy protection.

8.30 At the meeting of the Panel on Constitutional Affair of Legislative Council held on 15 December 2008, Legislative Council members queried on the deficiency of the Ordinance in enabling disclosure of personal data in the public interest. This proposal serves as a possible solution for the Administration's consideration.

8.31 The below examples show clearly the problems faced by data users when no such exemption exists:-

Example 1

In early February 2007, there were reports of incidents of failed Octopus EPS add-value transactions where Octopus cardholders failed to add value to their cards although monies were deducted from their bank accounts. Following the incidents, the Octopus Card Company identified a number of affected transactions and sought assistance from EPS Company (Hong Kong) Ltd to make the necessary refund. It was however discovered that the bank accounts of some of the affected cardholders have been closed and the cardholders could not be located. While some other banks may have the new contact information of the affected persons, it would be in breach of DPP3 to disclose the information to the Octopus Card Company. Should the PCPD be conferred with the power as proposed,

it would be a justifiable case for making a determination.

Example 2

In 2006, the Secretary for Health, Welfare and Food decided to develop an organ donation computer database by the Central Organ Donation Registry to facilitate people registering as organ donors and to boost up the number of registered donors in Hong Kong. The Hong Kong Medical Association (HKMA) since 1994 had kept some 40,000 registered organ donors in its database. It would therefore be necessary for HKMA to release its own database to the Central Organ Donation Registry. In order to comply with DPP3, it would be necessary for the HKMA to seek consent from the relevant registered donors. However, it might not be practicable to seek their consents as contact details of the registered donors were not up to date. Should the PCPD be conferred with the proposed power to make public interest determination, it will be a justifiable case for the PCPD to exercise his discretion.

8.32 A practical advantage of adopting this approach than a general public interest exemption is that the PCPD may impose controls on the act or practice to be conducted or engaged in so as to tailor-made the case to maintain public interest at the minimal scarification of personal data privacy. For instance, a decision to allow the disclosure of personal data may saddle the data user with a prohibition in disclosing certain kind of data, such as identity card number or name. Instead of making a blanket public interest exemption, the proposed scheme represents a gradual process whereby the PCPD is charged with the function to determine in each and particular case whether there is justifiable overriding public interest that outweighs the data privacy right of individuals.

8.33 On the basis of the above, the PCPD urges the Administration to take on board the proposal.

Public Domain Exemption

8.34 This proposal[56] originated from the PCPD concerns the creation of a new exemption from DPP3 in respect of personal data available in the public domain. While the PCPD is open-minded to the proposal, the Administration does not see a case to take this proposal forward.

8.35 Currently, personal data gathered or obtained from the public domain by a data user are treated no differently from other personal data under the current provisions of the Ordinance. Personal data can be made known in the public domain by various means, such as by being contained in public records and obtainable through public search or inspection, e.g. court documents filed, records kept by public registries, etc. Another means is by way of publication in the media, such as a journalistic report or a public announcement. Question arises as to whether a data user is still required to observe the requirements under DPP3 where the personal data are available in the public domain.

8.36 The PCPD acknowledges that there are problems of using publicly available information for secondary purposes, such as 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. Added to this is 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 a judgment debt against him.

8.37 It is therefore timely to consider whether personal data available in the public domain should be exempted from the data protection principle3.

[56] See PCPD's Proposal No. 36 in the Annex to the Information Paper.

Power to Search and Seize Evidence
Power to Call upon Public Officers for Assistance

8.38 These two proposals are bundled with Proposal No. 4 to confer power on the PCPD to carry out criminal investigation and to institute prosecution. Readers are invited to refer to PCPD's submissions made in paragraphs 4.2 to 4.11 above.

Power to Conduct Hearing in Public

8.39 This proposal to conduct hearing in public[57] was originated from PCPD but the Administration does not see there is a need to pursue.

8.40 Section 43(2) of the Ordinance provides that any hearing for the purpose of an investigation shall be carried out in public unless the PCPD considers otherwise or the complainant requested that the hearing be held in private. If the complainant's request is so received, under the current provision, the PCPD has no alternative but to accede to the request.

8.41 The PCPD finds the provision too restrictive that hinders public hearing. In cases when issues of public interest and importance are involved, members of the public should have a right to know and to be informed.

8.42 It is raised in paragraph 26 in Annex 2 of the Consultation Document that the LRC was concerned that the prospect of a public hearing could act as disincentive to the lodging of a complaint. Besides, the PCPD is already empowered to publish a report on the result of investigation under section 48(2) of the Ordinance.

8.43 In PCPD's view, the LRC's concern can be addressed by making it a proviso in the proposed amendment that the PCPD is required to consider all the circumstances of the case including the request from the complainant for the hearing to be conducted in private. Moreover, the PCPD considers that, while section 48(2) of the Ordinance enables the

[57] See PCPD's Proposal No. 15 at p.46 in the Annex to the Information Paper.

PCPD to publish a report after completion of an investigation, a requirement under section 43(2) of the Ordinance that a hearing shall be carried out in public is to ensure that the proceedings are conducted in an open and fair manner. In the PCPD's opinion, the concerns to be addressed by sections 43(2) and 48(2) are different.

8.44 The PCPD therefore considers that there is a need to review the current provision to enhance the right of the public to know and be informed.

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

8.45 This proposal to shorten the data user's response period to a report to be published under the Ordinance from 28 days to 14 days was originally made by the PCPD.[58] The Administration does not consider it appropriate to take forward the proposal.

8.46 Generally speaking, the PCPD will choose to publish a report when he considers the case involving an issue of significant social or public interest, sometimes on matter which has already been widely reported by the media. The effectiveness of sending out the message through the report will be hampered or diminished if it is not being reported timely.

8.47 The length of the notice period to respond to a report to be published by the PCPD under section 48 was prescribed when the Ordinance was first enacted. The notice period of 28 days should be reconsidered in light of the rapid development in technology and telecommunication which has profoundly enhanced efficiency in the decision making process.

8.48 Since the right of the relevant data user to comment on the draft report extends only to advising on any exempted matter contained in the report but not the contents of the report in general, it is considered that the period of 28 days to be excessively long. The PCPD therefore finds it necessary to shorten the period to 14 days.

[58] See PCPD's Proposal No. 31 at p.90 in the Annex to the Information Paper.

Annex 3 to the Consultation Document - Miscellaneous Proposed Amendments to the Ordinance

Proposal No. 32 : Power to Obtain Information to Verify a Data User Return

9.1 This proposal was originally made by the PCPD[59] in order to confer power on the PCPD to obtain information from any person in order to verify the particulars in a data user return filed under section 14 of the Ordinance.

9.2 Pursuant to section 14 of the Ordinance, the PCPD may, by notice in the Gazette, specify a class of data users to submit data user returns. The data user return shall be in a specified form and shall contain the prescribed information sets out in Schedule 3 of the Ordinance. The prescribed information now covers name and address of the data user, the kind of personal data collected, the purposes of collection, the classes of transferees of the data, the places to which the data will be transferred outside Hong Kong and the name and address of the individual to whom data access request may be made. The particulars in the data user return are made available for public inspection pursuant to section 16 of the Ordinance.

9.3 At present, there is no express power conferred under the Ordinance on the PCPD to obtain information from any person to verify the particulars stated in the data user return. The PCPD therefore proposes that such express power be provided under the Ordinance so that when there are reasonable grounds for believing that any particulars stated in the data user return are not true or accurate, the PCPD may exercise the power to obtain any information from any person to verify the particulars.

9.4 Apart from this proposal, the PCPD has also proposed to empower the PCPD to specify, from time to time, the "prescribed information" required to be submitted by a data user in a data user return. It will give more flexibility to the disclosure mechanism in a data user return, taking into account the changing needs and aspiration of privacy protection. Take the recent series of data security breaches as an

[59] See PCPD's Proposal No. 44 at p.126 in the Annex to the Information Paper.

example, if the proposal is taken on board, the PCPD may by notice in the Gazette, require a data user to include in the data user return information relating to data security breach. The proposal will increase the transparency of the data protection policies and practices adopted by data users and provide effective and efficient dissemination of the information to the general public. Individuals' trust and confidence on data users' determination to protect personal data privacy will be much enhanced which will ultimately benefit the data users in building up their reputation. Nowadays, transparency and accountability of data users are the focus of privacy governance. In order to face the challenge to personal data privacy in this electronic age, data protection must be robust, yet flexible. The PCPD therefore urges the Administration to pursue this proposal.

Proposal No. 36: Definition of Crime under Section 58

9.5 This was a proposal originated from PCPD[60] for the purpose of clarifying the scope of application of the exemption provision under section 58 by defining the word "crime". The Administration has made modification to the definition proposed by PCPD.

9.6 The Ordinance as it currently stands does not define the words "crime", "offenders" or "unlawful conduct" which are found in the exemption provision of section 58 of the Ordinance. Doubts were cast on the ambit of the exemption provision under section 58 of the Ordinance as to whether it is wide enough to cover overseas crimes and offences so that a data user can properly invoke the exemption in disclosing personal data to an overseas law enforcement agency for investigation of a foreign crime. It is therefore the aim of the proposal to clarify the scope of the application of the exemption.

9.7 In Hong Kong, the Mutual Legal Assistance in Criminal Matters Ordinance, Cap 525 ("MLAO") regulates the provision and obtaining of assistance in criminal matters between Hong Kong and places outside Hong Kong. Section 5(1)(g) of the MLAO provides that "a request by

[60] See PCPD's Proposal No. 3 at p.12 in the Annex to the Information Paper.

a place outside Hong Kong for assistance under this Ordinance shall be refused if, in the opinion of the Secretary for Justice, the request relates to an act or omission that, if it had occurred in Hong Kong, would not have constituted a Hong Kong offence".

9.8 The PCPD finds important public policy consideration when construing "crime", "offenders" or "unlawful conduct" in section 58. Having regard also to the territorial principle of the Ordinance, the PCPD considers it sensible, prudent and reasonable to interpret the words "crime" or "offenders" under section 58(1)(a) and (b) to mean "(i) an act or omission that is punishable as an offence under the laws of Hong Kong or (ii) an act or omission for which legal assistance under the Mutual Legal Assistance in Criminal Matters Ordinance, Cap 525 has been sought and obtained". And the criminal aspect of the meaning of "unlawful conduct" should be construed accordingly. The Administration's proposal modifies the PCPD's original proposal by replacing the meaning in (ii) by "a crime and offence under the law of a place outside Hong Kong, which is the subject of legal or law enforcement cooperation".

9.9 In this respect, the PCPD notes that under the MLAO, a territory will have to enter into an agreement with the Government of the HKSAR in relation to legal or law enforcement cooperation on criminal matters. By an order made by the Chief Executive in Council, the MLAO shall be made applicable as between the HKSAR and such territory subject to modification. A request for legal assistance in criminal matters has to be made to the Secretary for Justice and should satisfy the requirements specified under the provisions of the MLAO.

9.10 On careful examination of the wordings proposed by the Administration in the definition, the PCPD notes that there is no express reference to the request for assistance being made and obtained under the MLAO. This raises the concern that it may leave rooms for a local data user to rely on the relaxed exemption to disclose personal data to overseas authorities irrespective whether a request has been made to the Secretary for Justice for legal assistance under the MLAO. Such relaxation is not desirable from the perspective of personal data protection. In order to strike a proper balance between personal data privacy and investigation of crime,

the PCPD recommends the Administration to modify their proposal so that the definition will expressly refer to a request for assistance sought and obtained under the MLAO.

Other Proposals

10.1 The above submissions are made in respect of proposals which are more controversial in nature. The PCPD supports other proposals stated in the Consultation Document as listed in the Schedule attached. References to the corresponding proposals originally made by the PCPD are stated in the footnotes. Readers may refer to the relevant PCPD's original proposals in the Information Paper to better understand the underlying reasons for proposals.

- END -

III. Schedule

The PCPD supports the below proposals:-

Proposal No.	Brief Description
15	Access to Personal Data in Dispute[61]
16	Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation[62]
17	Erasure of Personal Data[63]
18	Fee Charging for Handling Data Access Requests[64]
19	Response to Data Access Requests in Writing and Within 40 Days[65]
24	Transfer of Personal Data in Business Mergers or Acquisition[66]
25	Provision of Identity and Location Data on Health Grounds[67]
26	Handling Personal Data in Emergency Situations[68]
28	Relieve PCPD's Obligation to Notify the Complainant who Has Withdrawn his Complaint of Investigation Result[69]
29	PCPD to Disclose Information in the Performance of Functions[70]
30	Immunity for PCPD and his Prescribed Officers from being Personally Liable to Lawsuit[71]

61 See PCPD's Proposal No. 25 at p.70 in the Annex to the Information Paper.
62 See PCPD's Proposal No. 23 at p.65 in the Annex to the Information Paper.
63 See PCPD's Proposal No. 43 at p.124 in the Annex to the Information Paper.
64 See PCPD's Proposal No. 26 at p.73 in the Annex to the Information Paper.
65 See PCPD's Proposal Nos. 21 and 55 at p.61 and p.146 respectively in the Annex to the Information Paper.
66 See PCPD's Proposal No. 38 at p.111 in the Annex to the Information Paper.
67 See PCPD's Proposal No. 32 at p.92 in the Annex to the Information Paper.
68 See PCPD's Proposal No. 34 at p.99 in the Annex to the Information Paper.
69 See PCPD's Proposal No. 48 at p.131 in the Annex to the Information Paper.
70 See PCPD's Proposal No. 30 at p.87 in the Annex to the Information Paper.
71 See PCPD's Proposal No. 18 at p.52 in the Annex to the Information Paper.

31	Power to Impose Charges for Educational and Promotional Activities[72]
33	Use of Personal Data Required or Authorized by Law or Related to Legal Proceedings[73]
34	Transfer of Records for Archival Purpose[74]
35	Refusal to Comply with a Data Access Request on Ground of Self-Incrimination[75]
37	Expand the Definition of "Relevant Person"[76]
38	Exclude Social Services from the Definition of "Direct Marketing"[77]
39	Exemption for Personal Data Held by the Court or Judicial Officer[78]
40	Extend Time Limit for Laying Information for Prosecution[79]
41	Duty to Prevent Loss of Personal Data[80]
42	PCPD to Serve an Enforcement Notice together with the Results of Investigation[81]
43	Contact Information about the Individual Who Receives Data Access or Correction Requests[82]

72 See PCPD's Proposal No. 9 at p.30 in the Annex to the Information Paper.
73 See PCPD's Proposal No. 35 at p.103 in the Annex to the Information Paper.
74 See PCPD's Proposal No. 37 at p.109 in the Annex to the Information Paper.
75 See PCPD's Proposal No. 22 at p.63 in the Annex to the Information Paper.
76 See PCPD's Proposal No. 4 at p.15 in the Annex to the Information Paper.
77 See PCPD's Proposal No. 28 at p.83 in the Annex to the Information Paper.
78 See PCPD's Proposal No. 7 at p.24 in the Annex to the Information Paper.
79 See PCPD's Proposal No. 17 at p.50 in the Annex to the Information Paper.
80 See PCPD's Proposal No. 56 at p.149 in the Annex to the Information Paper.
81 See PCPD's Proposal No. 49 at p.133 in the Annex to the Information Paper.
82 See PCPD's Proposal No. 42 at p.122 in the Annex to the Information Paper.