PCPD's Submission

in response to

Report on Public Consultation 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

I. Executive Summary

1.1 It has been over a decade since the Personal Data (Privacy) Ordinance (Cap. 486) ("**the Ordinance**") came into force on 20 December 1996. In 2006, the Office of the Privacy Commissioner for Personal Data ("**PCPD**") commenced a review of the Ordinance, taking into account the following factors:-

(a) the sufficiency of protection and the proportionality of penal sanction under the Ordinance;

(b) the development of international privacy laws and standards since the operation of the Ordinance;

(c) the regulatory experience of PCPD gained over the years;

(d) the technical problems encountered by PCPD in the application of certain provisions of the Ordinance;

(e) the technological development in an electronic age facilitating the collection, holding and processing of personal data in massive quantum at a low cost;

(f) the development of biometric technology for the identification of an individual posing challenges to the maintenance of individuals' privacy; and

(g) the vulnerability of individuals in becoming less able to control and determine the collection, use and security of his personal data stored and transmitted through electronic means.

1.2 In December 2007, the Privacy Commissioner for Personal Data ("**the Commissioner**") provided the Constitutional and Mainland Affairs Bureau ("**CMAB**") with a comprehensive package of over 50 proposals to amend the Ordinance.

1.3 On 28 August 2009, CMAB released the Consultation Document on Review of the Ordinance and solicited public views on various legislative amendment proposals, many of which originated from PCPD. The public consultation ended on 30 November 2009.

1.4 In response to the consultation exercise, the PCPD has prepared and submitted to CMAB in November 2009 a paper entitled *"PCPD's Submissions to Consultation Document on Review of the Personal Data (Privacy) Ordinance"* ("**PCPD's Submissions on the Consultation Document**") setting out PCPD's points of view on various proposals. The PCPD's Submissions on the Consultation Document has been uploaded to PCPD's website.[1]

1.5 On 18 October 2010, CMAB released the *"Report on Public Consultation on Review of the Personal Data (Privacy) Ordinance"* ("**the Consultation Report**") setting out the views received and the Administration's proposed way forward on its various proposals, including some new proposals to strengthen the protection of personal data used for direct marketing purposes.

1.6 The Commissioner notes that the Administration intends to pursue many of PCPD's proposals submitted earlier with a view to providing greater protection to personal data privacy, and enhancing the effectiveness and efficiency of PCPD's operations.

1.7 However, the Commissioner is concerned from reading the Consultation Report that some of the key proposals to step up protection of personal data privacy would not be pursued or taken forward by the Administration. The differences in view between the Administration and the PCPD are significant. The Commissioner notes that except for the proposals connected with the use of personal data for direct marketing purposes, the Administration's conclusions in the Consultation Report are largely based on the public and stakeholders' views collected more than a year ago. The Commissioner considers that after the *Octopus* incident, public demand and support were overwhelming for greater personal data protection and strengthening of PCPD's sanctioning

[1] Available at http://www.pcpd.org.hk/english/review_ordinance/files/PCPD_submission_ReviewPDPO_e.pdf.

powers. To meet the public's rising expectations and to align Hong Kong's data protection regime with international standards, the Commissioner is of the view that the PCPD's proposals shelved by the Administration should be resurrected. At least, they should be presented anew to the public for reconsideration.

1.8 To encourage different stakeholders and members of the public to give their views and opinions in this connection on the review of the Ordinance, the PCPD has embarked on a short but intensive public engagement exercise, with the Commissioner and his team meeting with stakeholders and interested parties as far and as much as practicable. The opportunity was taken to explain, in particular, the PCPD's stance on and the justifications for some major PCPD's proposals on which its view and that of the Administration is significantly different in whether or not they are worthy of pursuing. The PCPD attended a total of 41 public forums and meetings with interested parties for this purpose in the two-month consultation period.

1.9 This Submission sets out the PCPD's response to some of the amendment proposals in the Consultation Report. Many of the PCPD's views expressed in this Submission are reiteration and reinforcement of its views previously stated in the PCPD's Submissions on the Consultation Document. Some public worries and misconceptions made known to the PCPD were addressed. Further, objections to PCPD's proposals were commented on. Part II(A) concerns proposals that would be taken forward by the Administration while Parts II(B) & II(C) concern PCPD's proposals that the Administration would not take forward or pursue.

1.10 The PCPD has made an attempt to ascertain the level of public and stakeholders' sentiment and support to some of the PCPD's proposals shelved by the Administration, namely, the (1) to set up a territory-wide Do-not-call Register for person-to-person telemarketing calls, (2) to afford a higher protection to "Sensitive Personal Data", (3) to empower the PCPD to Award Compensation to Aggrieved Data Subjects, (4) to empower the PCPD to Impose Monetary Penalty on Serious Contravention of Data Protection Principles, and (5) to impose Direct Regulation on Data Processors and Sub-contracting Activities. A

questionnaire was sent to the parties and individuals who had made submissions to the Administration in the previous consultation exercise or had approached the PCPD and expressed their concerns during the recent consultation. An on-line survey was also launched from 8 to 28 December 2010 for the public to respond. Support for PCPD's proposals are identified, as explained in Part II of this Submission under various specific proposals. Detailed findings of the surveys are also analyzed in Part III herein.

Office of the Privacy Commissioner for Personal Data
31 December 2010

II. PCPD's Response to the Consultation Report

(A) Proposal to be Taken Forward by the Administration

Direct Marketing and Related Matters

Proposal 1 : Collection and Use of Personal data in Direct Marketing

2.1 In light of the widespread concerns in the community about the transfer of customers' personal data by some organizations for direct marketing purposes, the Administration has formulated this proposal to enhance the protection of personal data privacy in direct marketing activities.

Additional requirements and new offence

2.2 The PCPD supports the Administration's proposal to introduce additional specific requirements on data users who intend to use (including transfer of) personal data for direct marketing purposes as outlined in paragraph 3.2.32 of the Consultation Report.

2.3 The PCPD also supports that non-compliance of the aforesaid specific requirements will be made subject to the issuance of an Enforcement Notice; and that a new offence will be introduced for non-compliance (as stated in paragraph 3.2.35 of the Consultation Report). The Enforcement Notice issued by the PCPD is essential in directing data users to take remedial steps. On the other hand, the imposition of an offence will generate a direct deterrent effect on a data user.

More specific words needed in formulating the offence

2.4 With regard to the offence as set out in paragraph 3.2.35 of the Consultation Report, it will be difficult to prove (if it is made an element of the offence) that the presentation of the Personal Information Collection Statement setting out the intended direct marketing activities, the classes of persons to whom the data may be

transferred and the kinds of data to be transferred is not "*understandable and reasonably readable by the general public*". More specific words should be used to ensure that prosecution on the proposed offence could be brought with certainty.

Penalty level

2.5 While a higher penalty level will achieve the necessary deterrent effect for the proposed new offence, the PCPD recognizes that penalty levels should be 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.

2.6 The PCPD welcomes the Administration's proposed increase of the penalty level for contravention of section 34(1)(b)(ii) of the Ordinance to the level as proposed in paragraph 3.2.18 of the Consultation Report (i.e. maximum fine at $500,000 and imprisonment for 3 years). The PCPD also agrees that the maximum penalty for contravention of the new offence under this proposal be fixed at the same level.

2.7 In response to comments that the raised penalty may be too high, it should be noted that this merely represents the maximum penalty level. The Court will determine the appropriate penalties according to the circumstances of individual cases.

Transitional period and Grandfathering

2.8 It is unclear in the Consultation Report as to (1) whether a transitional arrangement will be introduced, and (2) whether data users will be required to comply with the new requirements with regard to the personal data collected before the commencement of the new provision.

2.9 From personal data privacy protection perspective, the PCPD advocates that data users should be required to comply with the additional specific requirements with regard to the personal data collected before the commencement of the additional provision.

Having regard to the likely problems that data users will have to cope in complying with the new requirements, the PCPD takes the view that a transitional arrangement is appropriate and sufficient time should be allowed for data users to comply with the new requirements.

Proposals not taken forward

2.10 It is noted that the new requirements proposed by the Administration only apply in situations where data users have obtained personal data directly from the data subjects but not where personal data are obtained from other sources. The PCPD urges the Administration to re-consider the following proposals to strengthen the regulatory regime on the use of personal data for direct marketing purpose.

(a) "Subscribed" or "Opt-in" approach

2.11 Paragraph 3.2.19 of the Consultation Report states that proposal (b) (the "subscribe" or "opt-in" proposal) will add burden to the operations of enterprises carrying out direct marketing activities, and proposal (c) (setting up a territorial-wide Do-not-call register to regulate person-to-person telemarketing calls in direct marketing activities) goes beyond the protection of personal data privacy.

2.12 In the experience of the PCPD, many of the complaints received concerns the use of personal data in person-to-person telemarketing calls that cause nuisance to the complainants. The Consultation Report relied on the opinion surveys conducted by the Office of the Telecommunications Authority ("**OFTA**") in 2008 and 2009 to say that around half of these calls did not involve the use of the recipients' personal data. It is to be noted that in the public opinion survey conducted by OFTA, 55% of the respondents reported that more than 40% of the person-to-person telemarketing calls received by them involved the use of personal data[2]. Also, a similar result was obtained by OFTA's industry survey which showed that 45% of such calls involved the use of the recipients' personal data[3]. Although it can be said that around half of such person-to-person telemarketing

[2] Paragraph 10 in LC Paper No.CB(1)240/09-10(04).

[3] Paragraph 10 in LC Paper No.CB(1)240/09-10(04).

calls do not involve the use of personal data, the figures may be interpreted the other way round to suggest that the use of personal data in these activities is prevalent. Furthermore, the surveys were conducted in 2008 and 2009. After the *Octopus* incident, public must have greater aspirations for privacy and less tolerance for unsolicited marketing calls.

2.13 Besides, there are clear voices expressed in the consultation exercise that the activities involving the collection and use of personal data for direct marketing purposes should be more tightly regulated. Measures should therefore be introduced to regulate these activities now. While the Administration has made a new proposal to strengthen the regulation on the collection and use of personal data in direct marketing activities, an "opt-out" approach is adopted in that the customers are invited, at the time when they provide their personal data to organizations, to "opt-out" from direct marketing approaches.

2.14 To protect the consumers' right of self-determination on the use of their personal data, PCPD's position is that an "opt-in" regime should be adopted in the long run requiring direct marketers to seek their explicit consent for the use of personal data for direct marketing purpose. This is consistent with the overwhelming public views expressed in consequence of the *Octopus* incident.

2.15 Insofar as overseas experiences are concerned, the "opt-in" approach has been adopted in the regulatory regimes of direct marketing with respect to fax, emails and automatic devices in the United Kingdom, Canada, the United States and France. Germany goes even further by subjecting telemarketing across-the-board (that is, including person-to-person telemarketing calls) to opt-in consent. The German Parliament also approved in 2009 penalties up to €50,000 for failure to obtain such consent prior to contacting consumers.[4]

2.16 The PCPD is aware of the concerns of direct marketers including the direct and immediate effect that an opt-in regime would cause on the

[4] Details can be found in a paper submitted by the PCPD to the Legislative Council on Overseas Regulatory Regime on Direct Marketing (available at http://www.legco.gov.hk/yr10-11/english/panels/ca/papers/ca1220cb2-582-4-e.pdf).

employment of telemarketers. Hence PCPD is amenable and receptive to pragmatic interim arrangements in moving to an "opt-in" regime.

(b) Setting up a territorial-wide "Do-not-call" register for person-to-person telemarketing calls

2.17 Given that it would take time for the direct marketers to shift to an "opt-in" regime and that unsolicited telemarketing calls are the most annoying nuisance to many consumers, the setting up of a territorial-wide "Do-not-call" register on person-to-person telemarketing calls is an ideal transitional arrangement that provides a win-win to both direct marketers and consumers.

2.18 Under this proposal, consumers may "opt-out" by registering their personal data (i.e. names and telephone numbers) in a central "Do-not-call" register operated by the Government. Telemarketers making calls to selected consumers would need to check this register beforehand and it would be an offence for them to make unsolicited calls to registered consumers against their opt-out wish. This proposal has the following benefits:-

- Recognizes that the existing arrangement for consumers to opt out of direct marketing approaches under section 34 of the Ordinance is deficient in that:-
  - they can only opt out after the approach has been made;
  - they have to exercise the option against each and every direct marketing company as the approach is made; and
  - they have to rely on the direct marketers to honour their unsubscribe requests[5].
- Provides an option for consumers to opt out of all unwanted telemarketing calls at the outset;
- Enhances the cost-effectiveness of telemarketing by avoiding approaches to consumers who would in any event reject the calls[6];

---

[5] According to a consumer survey commissioned by OFTA in October 2008, only 21% of the respondents said that callers would honour their requests.

[6] According to the same survey by OFTA, 43% of consumer respondents, when receiving person-to-person telemarketing calls, would indicate to the caller at the very beginning that they were not interested.

and

- Upgrades the image of the telemarketing industry and improves the morale of the telemarketers by eliminating calls that would definitely be regarded as nuisance.

2.19 This PCPD's proposal stems from the PCPD's experiences gained from handling complaints which involve both cold calls (without involving personal data) and targeted calls (involving personal data).

2.20 It is to be noted that a central do-not-call register has already been set up in the United Kingdom, Australia, Canada, New Zealand, France and the United States to prohibit unsolicited telemarketing calls (including person-to-person marketing calls) to be made to a number duly registered with the register.[7]

2.21 However, the PCPD recognizes that under the Unsolicited Electronic Messages Ordinance ("**UEMO**"), OFTA is already operating a "Do-not-call" register prohibiting the sending of commercial electronic messages to any telephone or fax number registered unless consent has been given by the registered user of the relevant telephone or fax number. The PCPD proposes therefore that OFTA's "Do-not-call" register should be expanded to include person-to-person telemarketing calls. Public support for this proposal was found in the two recent surveys conducted by the PCPD: see paragraphs 12.2-12.4, 12.11-12.13, 12.17-12.18, and 12.21.

2.22 The operation of "Do-not-call" register mainly depends on the registration of telephone numbers. A telephone number by itself (without one's name or other information) is not personal data as such because it is not possible to ascertain from the telephone number alone an individual's identity. The PCPD recognizes that this issue cannot be resolved merely by regulating the use of personal data in direct marketing under the Ordinance. It therefore urges the Administration to take up the matter with the OFTA without delay, with a request to include person-to-person telemarketing calls in its existing

[7] Details can be found in a paper submitted by the PCPD to the Legislative Council on Overseas Regulatory Regime on Direct Marketing (available at (http://www.legco.gov.hk/yr10-11/english/panels/ca/papers/ca1220cb2-596-1-e.pdf)

"Do-not-call" register.

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

2.23 In PCPD's original proposal, the Administration was urged to impose an obligation on a direct marketer to disclose the source of the personal data upon the data subject's request.[8]

2.24 The Australian Law Reform Commission made a similar recommendation in its Report 108 – For Your Information: Australian Privacy Law and Practice ("**ALRC Privacy Report**"). The Australian Law Reform Commission's view is extracted below:-

> *"Such a requirement would be useful particularly where an individual's personal information has been disclosed by an organization to another organization and it has then been used to carry out unsolicited direct marketing. In such a situation, the individual could follow a 'chain' of disclosure to the source and, if he or she wished, could then take action to have his or her name removed from the list. This would facilitate individuals being able to assert substantive, as distinct from merely formal, privacy rights with respect to direct marketing."*[9]

2.25 In this regard, the Australian Government has accepted the recommendation that individuals should have the right to be so informed by the organization if they have not had a customer relationship with the organization.[10]

---

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

[9] See paragraph 26.136 of the ALRC Privacy Report (available at http://www.alrc.gov.au/publications/26.%20Direct%20Marketing/content-%E2%80%98direct-marketing%E2%80%99-principle).

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

2.26 Furthermore, the PCPD has handled many complaints relating to direct marketing whereby the complainants experienced difficulties in tracing the source of their personal data from the direct marketers so as to enable them to stop future direct marketing approaches.

2.27 To implement the Administration's new proposals on direct marketing and Proposal 2 (Unauthorized Sale of Personal Data by Data User), it is even more pertinent to require a direct marketer to disclose the source of their personal data when so requested by a data subject. It will facilitate the data subject to trace the culpable parties who improperly disclose or sell his personal data against the originally-stated purpose of data collection and to lodge complaints on suspected commission of these new offences by the relevant data users.

2.28 It has been argued that data users will have great difficulties in complying with such requirements because the sources may be untraceable and it may add operation cost to direct marketers. This is not a valid or proper justification in refusing to confer such a fundamental right to individuals. Data users are expected to treat the collection, use and transfer of personal data seriously. Only if they fail to do so will source of data be untraceable. If for historical reasons the PCPD's proposal cannot be implemented in the short run, the PCPD accepts imposing a transitional period.

2.29 With this proposal, data users will be obliged to keep proper record of how they acquire the personal data in question. It will also promote and encourage data users to engage in practices that fully comply with the requirements of the Ordinance.

Proposal 2 : Unauthorized Sale of Personal Data by Data User

2.30 The Consultation Report proposes to require a data user to comply with the requirements in paragraph 3.3.5 if it is to ***sell*** personal data (whether collected from the data subject directly by the data user or obtained from another source) to another party for a monetary or in kind gain.

The word "sell" should be given a wider meaning

2.31 It should be noted that very often a data user will not state explicitly in its contractual arrangement with a third party that the data user is going to *"sell"* the personal data. Instead, it might use other choice of words in order to get round the concept of sale. It is therefore pertinent that the meaning of the word ***"sell"*** in the proposal should be given a wide definition to cover the situations where data user has not parted with possession of the customers' personal data but merely *"shared"* the personal data with its business partners whether for monetary or in kind gain. In many situations involving direct marketing, data users often engage in certain contractual relationships with their business partners (such as insurance companies) and allow them to approach their customers as "agents". The telemarketers, who are the employees of the business partners, will be given the relevant personal data for the purpose of direct marketing of the goods and services of the business partners themselves. In the circumstances, copies of the personal data have already been transferred in a duplicate form even though the data users may still keep their customers' personal data.

2.32 In addition, the Administration should be mindful of some contractual arrangements the descriptions of which are couched in such terms that the return for monetary or in kind gain (often named as "commission" or "bonus") is predicated upon successful engagement of the customers to subscribe for the services or purchase the products marketed by the business partners. Moreover, in a cross-selling situation, some organizations' cooperation may involve the sharing of personal data of customers. Whether the outcome of these types of operation would be regarded as *"in kind gain"* should be clearly specified in the law.

More specific words needed in formulating the offence

2.33 With regard to the requirements as set out in paragraph 3.3.5(b) of the Consultation Report, it will be difficult to prove (if it is made an element of the offence) that the presentation of the notice to inform the

data subject about the sale (on the kinds of personal data to be sold and to whom the personal data will be sold) is not "*understandable and reasonably readable by the general public*". More specific words should be used to ensure that prosecution of the proposed offence could be brought with certainty.

"Opt-in model" should be adopted

2.34 With respect to paragraphs 3.3.5(c) of the Consultation Report, the Administration invites submissions on whether to adopt an "opt-in model" or "opt-out model". The PCPD supports the requirement for data user to obtain data subject's explicit and voluntary consent if the personal data are to be "sold" to another party for a monetary or in kind gain. An "opt-in model" is considered more appropriate in that the data subject's preference is made known explicitly and without doubt.

New offence

2.35 The PCPD supports the proposal to regulate tightly the "sale" of personal data by data users for direct marketing purpose. The recent *Octopus* incident may only be the tip of the iceberg of similar malpractices in related industries. The public has expressed clear voices that personal data should not be "sold" (or transferred) for a monetary or in kind gain in the absence of the proper notice to the customer and/or without his explicit consent. Furthermore, the proposal is consistent with the Administration's approach to single out a particular act or conduct that is serious in nature and make it an offence.

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

Scope of the offence

2.36 It is recommended in the Consultation Report that this proposal, which is modeled on section 55 of the *UK Data Protection Act*, should be

implemented. The new offence is much narrower in scope than section 55 of the *UK Data Protection Act 1998* which provides that it is an offence for any person who:

(a) Knowingly or recklessly, without the consent of the data controller, *obtains* or discloses personal data or procures such disclosure, unless any of the defences are applicable; or

(b) Sells or offers to sell the personal data so obtained.

The PCPD takes the view that the proposed confinement of the new offence only to *"disclosure of personal data so obtained for (i) profits or (ii) malicious purposes"* will limit the scope of protection.

Malicious purpose

2.37 As revealed from paragraph 3.4.14 of the Consultation Report, the public is concerned about the meaning of *"malicious purposes"*. Also, most of the respondents to the consultation agree that those defences provided under the *UK Data Protection Act* should be taken as references (paragraph 3.4.15 of the Consultation Report).

2.38 With regard to the meaning of *"malicious purposes"*, the Administration suggested (in paragraph 3.4.14 of the Consultation Report) to define it as *"with a view to gain for oneself or another, or with an intent to cause loss, which includes injury to feelings, to another"* by referring to section 161 of the Crimes Ordinance (Cap. 200) concerning the offence of *"access to computer with criminal or dishonest intent"*.

2.39 Under section 161(1)(a) to (d) of the Crimes Ordinance, a person who obtains access to a computer *"(a) with an intent to commit an offence; (b) with a dishonest intent to deceive; (c) with a view to dishonest gain for himself or another; or (d) with a dishonest intent to cause loss to another…"* commits an offence. The meaning of *"gain"* and *"loss"* under section 161(2) of the Crimes Ordinance is construed to cover not only gain or loss in money or other property, but also extends to any such gain or loss whether temporary or permanent.

2.40 The legislative history of section 161 of the Crimes Ordinance and its scope is thoroughly discussed in the case *HKSAR v. Tsun Shui-lun* [1999] 2 HKC 547. In *HKSAR v. Tsun Shui-lun*, whether the defendant genuinely believed he was morally justified in doing what he did is held irrelevant under section 161(1)(c) of the Crimes Ordinance. However, this may not be easily reconciled with the general and accepted opinion to introduce the defences under section 55 of the *UK Data Protection Act* which are to a large extent premised on the defendant's motives (e.g. the person acted for the special purposes, with a view to the publication by any person of any journalistic, literal or artistic material and in the reasonable belief that such act was justified as being in the public interest).

2.41 Consideration should be given to avoid any inconsistency of the definition of the element of the offence with the various defences under section 55 of the *UK Data Protection Act*.

Criminal sanction and civil remedy in tandem

2.42 In paragraph 3.4.17 of the Consultation Report, the Administration considered that imposing criminal sanctions would be more appropriate than to deal with the relevant situations by civil remedies. To enhance personal data protection, the PCPD considers that both criminal sanction and civil remedies should be provided for. They are not mutually exclusive or complete replacements for one another. In cases involving infringement of one's privacy right, a data subject may find civil remedy such as injunction relief more appropriate, particularly as the damages under section 66 of the Ordinance may sometimes be nominal and therefore inadequate to remedy the aggrieved data subject's sufferings.

2.43 The PCPD suggests that the right to claim civil remedy, such as injunction order, should be clearly and explicitly spelt out in the Ordinance. It is to be noted that there is specific provision under the relevant discrimination legislations (e.g. section 54(1) of the Family Status Discrimination Ordinance, Cap.527) in Hong Kong to confer an aggrieved person with the right to bring civil proceedings in the like

manner as any other claim in tort in the District Court and all such remedies shall be obtainable in such proceedings as would be obtainable in the Court of First Instance. It is also explicitly provided that the District Court shall have jurisdiction to provide any remedy or injunction. Furthermore, reference can be drawn to sections 55A and 98 of the *Australian Privacy Act 1988* whereby a complainant or the Australian Privacy Commissioner is entitled to enforce the Commissioner's determination on the complaint and the civil remedy available also includes an order for injunction.

Data Security

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

Indirect regulation is insufficient

3.1 It is the original proposal of the PCPD to bring data processors and sub-contractors into the regulatory regime under the Ordinance because the current definition of "data user" expressly excludes them by virtue of section 2(12). In order to deal with the existing loophole, the PCPD proposed a two-limb regulatory model:-

(a) that data processors and sub-contractors should receive **direct regulation** under the Ordinance; and

(b) that data users should be required to use **contractual or other means to secure their data processors and sub-contractors to comply** with the relevant obligations under the Ordinance.

3.2 The proposal of **direct regulation** by imposing separate obligations on data processors and sub-contractors to comply with Data Protection Principles ("**DPP**") 2(2) (retention), 3 (use) and 4 (security) is to require them to:-

(a) ensure that 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 their 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.

3.3 The PCPD is concerned that the proposal for data processors and sub-contractors to be put under **direct regulation** of the Ordinance is

not accepted by the Administration. In particular, the PCPD does not consider it sufficient protection by simply relying on data users to regulate their data processors or sub-contractors by way of contractual means. The implication for indirect regulation is that they will only suffer loss of businesses or face civil liability claims from the data users in case of non-compliance with the contractual means. The PCPD will not be able to regulate them directly, nor to investigate directly into the matter. Also, data subjects cannot bring a claim against them directly, in addition to the claim against the data users.

Overseas data protection laws

3.4 The regulatory regime of direct regulation on data processors has been promulgated in overseas data privacy protection laws for many years. For instance, the United Kingdom followed the *European Union Directive 95/46/EC* and the *UK Data Protection Act 1998* specifically provides for the definition of *"data processor"* which essentially means any person who processes the data on behalf of the data controller. Insofar as personal data are entrusted to the processor for processing, it shall assume the role of data controller.

Misconception

3.5 The Information Technology ("**IT**") sector has expressed concerns on the proposal of direct regulation. It should be noted that this proposal is not targeting data processors in the IT sector specifically. It includes outsourcing or sub-contracting agents operating in other sectors.

3.6 With regard to the concern expressed in the Consultation Report that data processors do not have any knowledge of the nature or the use of the data and the procedures involved in data processing are complicated, it is to be noted that the proposal does not require them to ascertain the original purpose/retention requirements for which the data were collected by the users of the services. They are only required to act properly with respect to the purpose/retention requirement for which the data **were entrusted** to the data processors or sub-contractors. These requirements must have been known before

any services can be offered by data processors and should not be overly onerous. Similarly, the security requirement they have to meet needs only to be commensurate with the types of services they offer.

Other concern

3.7 Another concern expressed is that direct regulation of data processors may encourage data users to get around the proposed regulation by entrusting the work to overseas contractors. It should be noted that PCPD's proposal on the direct regulation of data processors will not lessen the responsibility of data user. Currently, data users are already made liable for the act or conduct of their agents by virtue of section 65 of the Ordinance. There is, therefore, no incentive for data users to specially outsource the work to overseas contractors. On the contrary, they may find it more difficult to control or to monitor compliance of overseas contractors. Further, they may even prefer to entrust their work to local data processors as the proposed direct regulation will impose upon the data processors a legal obligation to maintain high standards of data protection, thus reducing the risk of insufficient protection which data users will have to bear as principals.

PCPD's view

3.8 Instead of giving up the whole idea of imposing direct regulation on data processors or sub-contractors as indicated by the Administration, the PCPD proposes that, based on PCPD's past experiences, the following types of data processors or sub-contractors should be brought under direct regulation as a start:-

(a) Agents that are entrusted with personal data to **process** on behalf of the data users, for instance, an IT contractor being engaged by a data user to develop and maintain systems that handle personal data on its behalf. The IT contractor that was entrusted with sensitive information concerning the complaints against police officers in the IPCC case who subsequently leaked the personal data on the Internet is a case in point.[11]

[11] The published report on IPCC case is available at http://www.pcpd.org.hk/english/publications/files/IPCC_e.pdf

(b) Agents that are engaged to **destroy** personal data. As was observed in a case handled by the PCPD, bank clients' records that were supposed to have been properly disposed of ended up as wrapping papers used by florists in markets. Another real example is found in a case where it was reported in the news that the contractor of a law enforcement agency did not properly shred confidential waste papers entrusted to them. Consequentially, the waste papers containing sensitive witness statements were sold as recycled paper.

(c) Agents that are engaged for the physical **transmission or delivery** of personal data, e.g. couriers. The risk involved is the loss of packages containing personal data.

3.9 During the consultation period, the PCPD approached the IT sector and explained the proposal to them in details. As a result, the PCPD notes that there are still reservations and objections from the IT industry but the IT professionals generally agree with the proposal [12].

3.10 Direct regulation on data processors and outsourcing activities is important as the data processors play an increasingly predominant role in processing personal information in this IT age. Immediate steps to place them under direct regulation are required instead of shelving the proposal of direct regulation as a whole.

Proposal 6 : Personal Data Security Breach Notification

3.11 The PCPD notes with disappointment that the Administration decided not to proceed with the proposal despite the public's general agreement to the introduction of a personal data security breach notification system (paragraph 3.7.20 Consultation Report).

---

[12] Their views were gathered from the second survey conducted by the PCPD which details are further explained in Part III of this paper.

Overseas data protection laws

3.12 Data security breach notification is nothing new in overseas jurisdictions. Apart from voluntary breach notification that is usually governed by guidelines in jurisdictions such as Australia and New Zealand, mandatory breach notification has already been promulgated in other overseas privacy jurisdictions. In the United States, over 30 States have incorporated in their state laws a duty to notify individuals of leakage of personal information. Canada has already introduced mandatory privacy breach notification by its *Bill 29 – Safeguarding Canadian's Personal Information Act*. Also, there is a recommendation in the Australian Law Reform Commission Report published in August 2008 (recommendation 51-1)[13] to amend the *Australian Privacy Act* to introduce mandatory data breach notification. Introducing mandatory data breach notification is the world trend.

Onerous burden?

3.13 In paragraphs 3.7.21 and 3.7.23 of the Consultation Report, it is mentioned that privacy breach notification is not yet mature and imposing the requirement may cause onerous burden on data users. However, the figures of data breach notifications received by the PCPD in recent years suggest otherwise. From 1 April 2008 to 15 December 2010, the PCPD received 80 notifications from both the private and public sectors. Recently, the PCPD issued the "*Guidance on Data Breach Handling and the Giving of Breach Notification*". A template is provided for data users to use in giving notifications. With the Guidance Note in place specifying the details to be provided in the notification, the PCPD does not find introduction of mandatory privacy breach notification premature, as suggested in the Consultation Report.

3.14 In order to be effective, the notification system has to be made mandatory. It is noted that there is solid support (as shown in the Consultation Report) to making the notification a mandatory requirement. For the avoidance of doubt, the PCPD has not proposed

[13] Available at: http://www.austlii.edu.au/au/other/alrc/publications/reports/108/51.html#Heading386

that each and every breach has to be notified. It reiterates the views in paragraphs 3.26 to 3.28 of the PCPD's Submissions on the Consultation Document that the mandatory notification requirement can be introduced by stages to ensure a gradual process for the implementation with reference to the factors such as the amount of data being held by the data users, the sensitivity of the data and the risk of harm that may be inflicted as a result of a security breach.

Statutory Powers and Functions of the Privacy Commissioner for Personal Data

Proposal 11 : Additional Grounds for Refusing to Investigate

4.1 In its original proposal, the PCPD proposed to introduce three additional grounds of refusal to carry out investigation as stated in paragraph 3.12.3 of the Consultation Report. It is noted that only ground (a) *"where the primary cause of the complaint is not related to personal data privacy"* is accepted by the Administration and will be included in section 39(2) of the Ordinance.

4.2 With regard to ground (b), i.e. *"where the complaint relates to any action which the complainant has a remedy in court or tribunal or which is currently or soon to be under investigation by another regulatory body"*, PCPD considers it will ensure that the limited resources under its disposal are not wasted through duplication of effort. As pointed out in the PCPD's Information Paper, similar provision can be found in section 10(1)(e)(ii) of the Ombudsman Ordinance (Cap. 397) to allow the Ombudsman not to undertake investigation if the complaint relates to any action in respect of which the complainant has or had a remedy in a court or in any tribunal by or under any Ordinance[14]. It is difficult to reconcile such disparity of treatment between the two statutory bodies that are vested with similar complaint handling functions and no justification can be found in the Consultation Report.

4.3 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 PCPD reiterates that such additional ground is necessary (the grounds are elaborated in paragraph 7.18 of the PCPD's Submissions on the Consultation Document). The classic example to illustrate the justification for this additional ground is where the complainant is engaging in fishing expedition to obtain documents and data (through the lodging of a data access request)

[14] Paragraph 12.3 on page 29 of the PCPD's Information Paper.

which he would otherwise only be entitled to under discovery procedures taken in legal proceedings.

4.4 This proposal was made following the decision in *Wu Kit Ping v. Administrative Appeals Board*, HCAL60/2007[15]. While the PCPD may seek to refuse to investigate this sort of cases by relying on section 39(2)(d) that *"any or further investigation is for any other reason unnecessary"*, an express provision of this additional ground (c) under section 39(2) of the Ordinance will help avoid unnecessary arguments and appeals to the Administrative Appeals Board ("**AAB**"). It should be noted that it is time-consuming and resources-draining to handle appeals lodged with the AAB.

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

4.5 It is noted that the proposal will only confer upon the Commissioner the power to obtain information from any person in order to verify the information in a data user return. In PCPD's original proposal[16], it is also proposed that the Commissioner be conferred with the power to specify, from time to time and by notice in the Gazette, the "prescribed information" to be reported in a data user return. While this proposal was not taken up by the Administration at the time of conducting the public consultation last year, it is timely to resurrect the proposal in the light of the recent *Octopus* incident which indicated there is high public expectation for greater transparency in handling personal data by enterprises.

4.6 The *Octopus* incident shows the general problem of data user providing personal data collection statements to customers in small prints and giving non-specific description of the classes of transferees of personal data. Under the data user return system, data users will be required to file returns containing the prescribed information and

---

[15] The Court stated that the purpose of the Ordinance is not 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 33.

[16] See proposal 44 page 126 of Annex to the PCPD's Information Paper.

the general public will be allowed to inspect the information free of charge. A data subject may inspect the particulars contained in a data user return before deciding whether or not to provide his/her personal data to the data user. It is clear from the *Octopus* incident that there is a high public expectation for more details to be provided by data users in using personal data for direct marketing purposes including the relevant types of personal data transferred for these purposes.

4.7 With the proposed power, the Commissioner may expand the prescribed information to be reported by notice in the Gazette from time to time by taking into account the changing needs and aspirations of the stakeholders. This is consistent with the open and transparent principle to keep the public informed of the collection and handling of their personal data by data users through the data user return system.

Offences and Sanctions

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

5.1 In paragraph 3.19.12 of the Consultation Report, it is proposed that the penalty for this new offence should be the same as that for non-compliance of an enforcement notice, i.e. a fine at Level 5 ($50,000) and imprisonment for two years.

5.2 The PCPD takes the view that a higher penalty level should be imposed taking into account the more culpable nature of repeated contraventions when compared with non-compliance of an enforcement notice. A data user who has repeatedly contravened a DPP on the same facts, even though an enforcement notice has not been issued, should be imposed with a higher penalty. According to the ranking table found in paragraph 5.22 (page 35) of the PCPD's Submissions on the Consultation Document, this new offence has a higher ranking than the non-compliance of an enforcement notice. For data users who are large organizations with ample financial resources, imposing a heavier fine is considered a more effective penalty than custodial sentence.

Proposal 19 : Repeated Non-compliance with Enforcement Notice

5.3 In paragraph 3.20.12 of the Consultation Report, it is proposed that committing this new offence will attract a fine at Level 6 ($100,000) with two years imprisonment and in case of a continuing offence, a daily fine of $2,000.

5.4 The PCPD takes the view that a higher penalty should be imposed taking into account the more culpable nature of such offence when compared with first-time non-compliance of an enforcement notice and the new offence of Repeated Contravention of a Data Protection Principle on Same Facts under Proposal 18 above. According to the ranking table found in paragraph 5.22 (page 35) of the PCPD's

Submissions on the Consultation Document, a higher ranking is given for this new offence.

Overall review of penalty level and director's liability

5.5 Furthermore, the overall penalty level of the various offences under the Ordinance should be reviewed to achieve greater deterrent effect for the protection of personal data privacy rights.

5.6 Currently, a director or other officer of an organizational data user may be prosecuted and made guilty of the offence under the Ordinance by virtue of section 101E of the Criminal Procedure Ordinance (Cap. 221) where it is proved that the offence was committed with the consent or connivance of a director or other officer concerned in the management of the company. However, that is not expressly spelt out in the Ordinance. Even though it does not alter the position under the current law, a new subsection to be inserted under section 64 of the Ordinance to spell out clearly such provision will explain the law in much clearer terms and thus help promote compliance with the requirements under the Ordinance by directors of organizational data users.

Rights and Obligations of Data Users

Proposal 23 : Response to Data Access Requests in Writing and Within 40 Days

6.1 The PCPD is not convinced of the justification given in the Consultation Report to grant exclusive exemption to the Police for responding to data access request in respect of criminal conviction record. Any exemption for a particular data user for complying with the proposed requirement should not be granted lightly. The justification mentioned in paragraph 3.24.3 of the Consultation Report is that *"citizens who cannot produce clear criminal conviction records may be labeled as 'underclass' citizens"*. The alleged labeling effect put forward as the sole reason for allowing exclusive relaxation to the Police on this new requirement is insufficient.

6.2 Insofar as the alleged labeling effect is concerned, the Police have been acceding to requests for integrity checks of potential employees from the Government departments and various public bodies for many years. It is evident that in some circumstances, it is necessary or justified for employers to be given access to such data for employment purpose. It also demonstrates that the labeling effect, if it exists at all, should be more properly addressed by looking into the root of the problem, i.e. whether any employer has infringed DPP1(1) of the Ordinance by unjustifiably obtaining clear conviction record from potential employees. If affirmative, such act of data collection would be excessive for the purpose of employment. This is a better approach than simply denying data subjects' right to access their own personal data which is a fundamental right of personal data protection.

Introducing New Exemptions

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

7.1 It is noted that this proposal, which is not originated from the PCPD, is to be taken forward in the Consultation Report. The PCPD's comments on this proposal can be found in paragraphs 6.21 to 6.24 in the PCPD's Submissions on the Consultation Document. The PCPD reiterates the opinions made therein, in particular:-

(a) 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 fulfill their responsibility to exercise proper care and guardianship of their children under the age of 18. In order that the transfer is justifiable, consideration should be given to the types of the exempted personal data, the degree of disclosure and the relevant circumstances at the material time. The types of the exempted personal data should be specifically defined and the data should also be limited to those that are necessary in the circumstances.

(b) A robust mechanism must be built in to guard against misuse.

(c) Minors who attain certain age should be allowed to make their own decisions in relation to the disclosure of the personal data.

(B) Proposal Not to be Taken Forward by the Administration

Harnessing Impact on Personal Data Privacy Caused by Technological Advancement

Proposal 38 : Sensitive Personal Data

8.1 The PCPD is disappointed that this proposal is not taken forward in the Consultation Report. The main reason for not taking this proposal forward is that different sectors of the community have not yet reached a consensus on the coverage of sensitive personal data and the regulatory model (paragraph 4.2.28 of the Consultation Report). However, most of the views expressed in the Consultation Report agreed with the general direction of providing a higher degree of protection to sensitive personal data (paragraph 4.2.26 of the Consultation Report).

Overseas data protection laws

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

8.3 In relation to the coverage of sensitive personal data, the *European Union Directive 95/46/EC* specifies *"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"* as sensitive personal data. The *UK Data Protection Act* generally follows the *EU Directive* and in addition to the types of personal data specified in the *EU Directive*, treats *"the commission or alleged commission of an offence and any proceedings relating to an offence alleged to have been committed"* as sensitive personal data. In

Australia, the Australian Law Reform Commission has recommended (as accepted by the Australian Government) to extend the definition of *"sensitive personal data"* to cover *"biometric information"* that is specifically being collected to identify or verify an individual through biometric processes[17].

Keeping up with International Standard

8.4 The PCPD's proposal to give special treatment for sensitive personal data is in accord with the *EU Directive*, 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 protection of personal data in the country to which the data will be transferred. Hence, adoption of the EU approach will ensure uninterrupted exchange of personal data with the EU member states which is conducive to sustain the growth in trade and business activities in Hong Kong.

Domestic Consideration

8.5 It is acknowledged that the classification of sensitive personal data is cultural bound and varies in different communities. According to the surveys conducted by the PCPD, the majority[18] of those who supported the proposal agreed that data concerning sex life, health condition and biometric data should be classified as sensitive personal data.

8.6 As for biometric data, the PCPD recognises that not every type of biometric data is sensitive. The PCPD advocates the inclusion of those data that can be used *to identify or authenticate* an individual through biometric processes as sensitive personal data[19]. Examples are fingerprints and genetic data. Unlike a password or a PIN which can be reset, they are very personal and private because they are unique information about an individual's physical self. The integrity of such data must be safeguarded to protect the individual's identity against

---

17 See the First Stage Response to the Australian Law Reform Report. Available at http://www.dpmc.gov.au/privacy/alrc_docs/stage1_aus_govt_response.pdf

18 Please refer to Part III of this paper

19 By adopting a similar approach as the Australian Law Reform Commission

theft or misappropriation.

8.7 As for data concerning sex life or sensitive health condition, the leakage of these data could embarrass or damage the reputation of the data subject. These data may provide basis for unjustified discrimination. For example, the wide dissemination of data concerning the sex life of some prominent artistes through the Internet a few years ago causing significant damage to the individuals concerned is a case in point. Furthermore, disclosure of data concerning one's health condition (e.g. HIV result) is highly privacy intrusive.

8.8 Instead of shelving the proposal as indicated by the Administration, the PCPD takes the views that the proposal should be taken forward. The surveys conducted by PCPD clearly identified strong support for classifying biometric data, health condition and sex life of individuals as sensitive personal data and affording them greater protection[20].

[20] As noted from the surveys result (in Part III), over 50% of the supporters consider that information concerning sex life and health condition, as well as biometric data, should be classified as sensitive personal data and given greater protection

Sanctioning Powers

9.1 The recent *Octopus* incident has seen the community up in arms demanding the punishment of data users for violation of the provisions under the Ordinance, reflecting clearly the gap between public expectations and the current sanctioning powers of the PCPD. Although the Administration finally decided to take forward the PCPD's proposal to relax the restrictions for the PCPD to issue enforcement notice under section 50 of the Ordinance (Proposal 8 – Circumstances to Issue Enforcement Notice), that alone is insufficient.

Proposal 39 : Granting Criminal Investigation and Prosecution Power to the PCPD (considered together with Annex 5 : Powers to Search and Seize Evidence and to Call upon Public Officers for Assistance)

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

9.3 The PCPD has no intention to usurp the Secretary of Justice's power or discretion to prosecute. The PCPD's proposal entails only the PCPD carrying out the prosecution work. The discretion whether or not to prosecute always is and shall remain reserved for the Secretary for Justice. Under PCPD's proposal, any prosecution to be initiated by the PCPD shall only be carried out with the consent of the Secretary for Justice. The power and function of prosecution, if vested with the PCPD, entail the due presentation of facts by the PCPD to the Court. It does not place the PCPD in a position to decide or judge the culpability of any data user. That power, as always, stays with the Judiciary.

9.4 Data protection and privacy is relatively narrow subject in law enforcement and criminal prosecution. The PCPD considers that its staff has the knowledge, experience and skills to undertake the associated criminal investigation and prosecution work. On the other

hand, it would be difficult for the Police and the Department of Justice to specialize in this area.

9.5 There are concerns that this proposed new role might conflict with the PCPD's existing role of community education and helping data users to comply with the requirements under the Ordinance. These worries could be addressed by organizational structuring. The PCPD could compartmentalize its investigation and prosecution team from the community education team.

9.6 It should be noted that the PCPD is an independent privacy enforcement authority. It is empowered under the Ordinance to investigate infringement of personal data privacy by both the public and the private sectors. Granting criminal investigation and prosecution powers to the PCPD will help avoid criticism of favouritism where the Police or other Government departments are involved in the case as data user. Indeed, based on PCPD's experience, some complainants prefer the cases to be handled by the PCPD rather than the Police. When asked to give consent for referral of complaint to the Police for criminal investigation, some complainants had refused to proceed further.

9.7 Another opposing reason given by the Administration is the small number of referrals and successful convictions in the past years which do not justify granting the power to the PCPD. It should be noted that whether or not to prosecute, or whether a prosecution results in successful conviction is not in the hands of the PCPD once a case is referred out. The fact is that cases of contravention of the 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.

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

Proposal 1 – Collection and Use of Personal Data in Direct Marketing
Proposal 2 – Unauthorized Sale of Personal Data by Data User
Proposal 3 – Disclosure for Profits or Malicious Purposes of Personal Data Obtained without the Data User's Consent
Proposal 18 – Repeated Contravention of a Data Protection Principle on Same Facts
Proposal 19 – Repeated Non-compliance with Enforcement Notice
Proposal 27 – the Offence on Misuse or Excessive Retention of Personal Data in Business Mergers or Acquisition

9.9 Further, 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.

9.10 The PCPD believes that it would be in the best interest of the community in terms of enhancement of personal data privacy protection to confer criminal investigation and limited prosecution powers on the PCPD. While the community might not be ready to support this proposal last year, the situation may be different now in consequence of the *Octopus* case which has highlighted the lack of sanctioning powers of the PCPD. The PCPD further considers that the following proposals to strengthen the sanctioning powers of the PCPD should be adopted to produce a greater effect to deter privacy contraventions.

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

9.11 The enforcement action to be taken against contravention of the DPP in Schedule 1 of the Ordinance is limited to serving on the relevant data user an enforcement notice pursuant to section 50(1) of the

Ordinance directing it to take steps to remedy the contravention. It is only when the data user fails to comply with the terms of the enforcement notice that the data user may then be prosecuted. Proposals 40 and 42, if adopted, will address the public concerns about the inadequacy of PCPD's sanctioning powers. They aim at compensating aggrieved data subjects and penalizing data users for blatant disregard of personal data privacy rights.

Both proposals are modeled on data privacy laws in other common law jurisdictions

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

Proposal 40

Adjudication / Conciliation

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

Australian examples on award of compensation and appeal

9.14 Modeled on the Australian system, the aggrieved data subject is usually only compensated for actual loss or damage. The onus is on the claimant to prove damages. For example, in one case in 1993, the Australian Privacy Commissioner declared that a complainant was entitled to AUD$5,000 as compensation for the embarrassment caused by the unauthorized disclosure of the complainant's employment record by his former employer[21]. In another case in 2003, the Australian Privacy Commissioner declared that a complainant was entitled to AUD$1,000 as compensation for the infringement of his privacy as a result of the disclosure of his identity to a third party and the complainant was also entitled to be paid certain part of his legal costs, traveling expenses and loss of income at AUD$1,643[22].

9.15 In the case *Re Alan Rummery and Federal Privacy Commissioner-BC200410810* [2004] AATA 1221, the Australian Administrative Appeals Tribunal considered an appeal against the Australian Privacy Commissioner's decision in refusing to make an award of compensation to the complainant. The complainant was subsequently awarded by the Tribunal with compensation AUD$8,000 for the loss and damage suffered.[23]

Legal Assistance is only granted under limited circumstances

9.16 It is mentioned in the Consultation Report that aggrieved data subjects would be given sufficient assistance to claim compensation under section 66 of the Ordinance by implementation of Proposal 7 (Legal Assistance to Data Subjects under section 66). However, it should be noted that Proposal 7 arrangements can only be selectively applied and cannot replace Proposal 40. According to the model of the Equal Opportunities Commission ("**EOC**") quoted in the Consultation Report, the relevant legislation empowers the EOC to accede to a

---

21 Available at http://www.privacy.gov.au/materials/types/determinations/view/6029.
22 Available at http://www.privacy.gov.au/materials/types/determinations/view/6792.
23 Available at http://www.austlii.edu.au/cgi-bin/sinodisp/au/cases/cth/AATA/2004/1221.html?stem=0&synonyms=0&query=Re%20Alan%20Rummery.

request for legal assistance under certain conditions only.[24] Applying the same conditions to legal assistance under the Ordinance, an aggrieved data subject will not be assisted unless any one of the prescribed conditions is fulfilled. The PCPD envisages that in the great majority of cases, the aggrieved data subject will not be given legal assistance and has to initiate civil action by himself. What he has to face is usually an organizational data user who has ample resources to contest the civil action.

Statutory provision for mediation

9.17 At present, there is no express provision under the Ordinance for the PCPD to carry out mediation of a complaint. The PCPD further proposed that an additional power be conferred on the PCPD to carry out mediation of a complaint including settlement by a monetary sum. If the relevant parties do not agree to the mediation by settlement, the PCPD may resort to the power of award of compensation. The PCPD takes the view that both Proposals 7 and 40 as well as the proposal on mediation should be taken on board in order to provide sufficient and efficient assistance to the aggrieved data subjects, thereby generating direct and effective deterrent effect on data users against infringement of the Ordinance.

Proposal 42

Overseas example

9.18 In circumstances involving serious and blatant disregard of the personal data privacy rights, the issuance of an enforcement notice directing data user to take remedial steps is considered insufficient. Proposal 42 (Empowering the PCPD to impose Monetary Penalty on Serious Contravention of Data Protection Principles) will equip the PCPD with the power to impose monetary penalty on the data user to achieve the necessary deterrent effect. By reference to the United

[24] The factors that have to be considered are (a) the case raises a question of principle, and (b) it is difficult for the applicant 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.

Kingdom model, the PCPD may serve on a data user a monetary penalty notice where the Commissioner is satisfied that (a) there has been a serious contravention of the data protection principles; (b) the contravention is of a kind likely to cause substantial damage or distress; and (c) the data controller knows or ought to have known a risk of contravention of a kind likely to cause substantial damage or distress but he failed to take reasonable steps to prevent the contravention. The decision on the service of a penalty notice is subject to an appeal. The amount of penalty to be determined must not exceed the maximum amount as prescribed. For reference, under the current UK legislation regime, the maximum monetary penalty that the UK Information Commissioner may impose is £500,000.

9.19 The UK Information Commissioner has issued a statutory guidance on the application of such power to impose monetary penalties and have recently exercised his power to issue penalty notices on data users in cases involving serious contraventions of the data protection principles. His power is not absolute. The statutory guidance has the approval of the Secretary of State before it takes effect.

9.20 In November 2010, the UK Information Commissioner invoked his newly-gained power to impose monetary penalties for serious data protection contraventions in two cases[25], the details of which are briefly outlined below:-

(1) The first penalty of £100,000 was issued for two serious incidents where the employees of a data user faxed highly sensitive personal information to the wrong recipients. The first case involved data on child sexual abuse. The second case involved the information related to care proceedings of 3 children, the previous convictions of two individuals, domestic violence records and care professionals' opinions. After the first breach, the data user did not take sufficient remedial steps and allowed the second breach to occur.

[25] Available at http://www.ico.gov.uk/~/media/documents/pressreleases/2010/first_monetary_penalties_press_release_24112010.ashx.

(2) The second monetary penalty of £60,000 was issued to another data user for the loss of an unencrypted laptop which contained personal information relating to 24,000 people who had used certain community legal advice centres. The personal information involved included full names, dates of birth, postcodes, employment status, income level, information about alleged criminal activity and whether an individual had been a victim of violence. Monetary penalty was considered necessary given access to the data could have caused substantial distress to the data subjects. Also, the data user did not take reasonable steps to avoid the loss of the data when it issued the employee with an unencrypted laptop, despite knowing the amount and type of data that would be processed on it.

Appropriate examples in Hong Kong for imposing monetary penalties on serious contraventions

9.21 As evident in the *Octopus* incident, there is a public demand to equip the PCPD with the power to impose monetary penalty to encourage compliance and to deter against serious contraventions on the part of data users. Examples of past cases that the proposed sanction might be invoked are:-

(a) The *Octopus* incident where personal data of more than 2 million members were transferred, without the members' voluntary and express consent, to third parties for monetary gains;

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

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

9.22 From the opinion surveys carried out by the PCPD in December 2010[26], one may conclude that the number of people supporting Proposals 40 and 42 is more or less the same as the number of people objecting. The proposals deserve further and serious consideration by the Administration.

[26] In Part III of this paper.

Others

Proposal 44 : Fee Charging for Handling data Access Requests

10.1 The Administration's decision of not adopting this proposal will be in direct conflict with Law Reform Commission's recommendation under paragraph 14.31 of the Report on Reform of the Law Relating to the Protection for Personal Data (1994). Pursuant to the report, it was recommended that the question of level of fees for complying with data access requests be provided for in subsidiary legislation. Such recommendation has not been adopted by the Administration since the commencement of the Ordinance.

10.2 The Proposal will introduce certainty and yet preserve flexibility to allow data users to charge differently. Section 28(3) of the Ordinance allows data users to charge fees that are not excessive for complying with data access requests. The Proposal will avoid unnecessary complaints against excessive fees if they are charged at the prescribed level provided under the proposed fee schedule. The items listed in the proposed fee schedule are not exhaustive. Any fees imposed otherwise in accordance with the fee schedule will still have to meet the existing requirement of not being excessive.

10.3 A similar approach of imposing a maximum fee is adopted in other overseas data privacy protection laws. In the United Kingdom, a data user is entitled to receive such fee not exceeding the prescribed maximum[27]. Locally, the PCPD also received comments and views from different public and private organizations in support of introducing a fee schedule for handling data access requests as this will create certainty of imposing charges without infringing the law. It is highly recommended that the Administration takes this opportunity to introduce a fee schedule.

[27] Section 7(2) Data Protection Act 1998. The prescribed maximum is set at £10 and there are special rules that apply to fees to be imposed on other kinds of access requests.

(C) Proposal Not to be Pursued by the Administration

Annex 5 : Territorial Scope of the Ordinance

11.1 This proposal is made by PCPD 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 outside Hong Kong. The Administration is not inclined to pursue the proposal.

11.2 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.

11.3 The justification and explanation for this proposal can be found in paragraphs 8.17 to 8.26 of the PCPD's Submissions on the Consultation Document and the PCPD's original proposal in the PCPD's Information Paper[28]. The PCPD is concerned that if the proposal is not taken on board, a person who is able to control his business operations overseas will be considered a data user subject to Hong Kong law by his mere presence in Hong Kong. It would be unfair to the person if the Hong Kong law and overseas law both govern the handling of the data not originated from Hong Kong, particularly where there is a conflict of laws situation.

Annex 5 : Power to Conduct Hearing in Public

11.4 The Commissioner has conducted a public hearing for the purpose of investigating the *Octopus* incident for reason that it involves significant numbers of data subjects and attracts huge public concerns. The effectiveness of conducting public hearing and its resultant educational value has been clearly illustrated.

11.5 However, under the existing provision of the Ordinance, if the complainant as a data subject requests a hearing to be conducted in

[28] See PCPD's Proposal No. 6 in the Annex to the Information Paper.

private (pursuant to section 43(2) of the Ordinance), the Commissioner has no alternative but to accede to the request. The PCPD finds the provision too restrictive and maintains that flexibility should be introduced to allow the Commissioner to decide whether a hearing should be conducted in public having regard to all the circumstances of the case and the objection from the complainant is one of the matters that the Commissioner should take into account.

11.6 The PCPD appreciates the argument that public hearing may in some cases dissuade complaints. However, when issue of public interest arises, conducting the hearing in public with the complainant to remain anonymous throughout the hearing may still serve the purpose of addressing the public's right to know and without compromising the interest of the complainant at the same time.

Annex 5 : Time Limit for Responding to PCPD's Investigation/ Inspection Report

11.7 The PCPD reiterates that the 28 days notice for a data user to respond to a report to be published under the Ordinance was prescribed when the Ordinance was first enacted. It should be reconsidered in light of the rapid development in technology and telecommunication, which has profoundly enhanced efficiency in a decision-making process.

11.8 Furthermore, in cases that involve public interest, it is justified for a swift response to be given to address the public concern. The PCPD noted that there are public sentiments in the *Octopus* incident that the 28 days period is too long for the relevant data user to respond. Additionally, it is undesirable that the Commissioner is required under the current provision in section 46(4) of the Ordinance to give the notice even though there is no personal data mentioned in the report. Time is wasted in order to comply with the formality. The Administration is urged to re-consider the proposed way forward.

III. Surveys Conducted by the PCPD

12.1 Despite limited resources and time constraints, the PCPD carried out 3 separate surveys to solicit public and stakeholders' views on five of its original proposals which the Administration has indicated not to pursue further, namely:-

(1) To set up a territorial-wide "Do-not-call" Register for person-to-person telemarketing calls (related to Proposal 1);
(2) Sensitive Personal Data (Proposal 38);
(3) Empowering the PCPD to Award Compensation to Aggrieved Data Subjects (Proposal 40);
(4) Empowering the PCPD to Impose Monetary Penalty on Serious Contravention of Data Protection Principles (Proposal 42); and
(5) To Impose Direct Regulation on Data Processors and Sub-contracting Activities (Proposal 5).

The outcome of the surveys is captured in the ensuing paragraphs.

Targeted Survey regarding Proposals 1, 38, 40 and 42

12.2 On 3 and 13 December 2010, the PCPD sent out to the following 95 targeted respondents a questionnaire on the above four proposals (except Proposal 5):-

(a) the parties and individuals who had made written submissions to the Administration in the consultation exercise in 2009[29]; and/or

(b) the stakeholders/academics who (i) had made written submissions to the Legislative Council Panel on Constitutional Affairs and/or attended its Special Meeting on 20 November 2010 in response to the Consultation Report, or (ii) had approached the PCPD and expressed their concerns during the recent consultation.

[29] The contacts of the individuals who had made submissions are not made public in the Consultation Report and the PCPD's questionnaire can therefore only be sent to those organizations and individuals whose names or contact addresses can be identified during the consultation 2009.

12.3 43 replies were received by the PCPD. In addition, 13 responses were unsolicited and the responses are incorporated in the results of the on-line survey (paragraphs 12.11-12.18 below), rather than included in the analysis below.

Setting up a territorial-wide "Do-not-call" Register for person-to-person telemarketing calls (related to Proposal 1)

12.4 18 respondents supported the proposal to set up a territorial-wide "Do-not-call" Register, against 11 respondents objecting. One respondent supporting the proposal pointed out that the proposal should be given a high priority even if this goes beyond the current framework of data privacy protection.[30] One respondent objecting to the proposal pointed out that large businesses and small-medium enterprises would be greatly disadvantaged through the imposition of a "Do-not-call" Register and suggested self regulation by the businesses concerned.[31] Another respondent considered that the existing Do-not-call registers operated by the OFTA have already afforded consumers with choices.[32] It is further pointed out that a Code of Practice was already issued for the members in the direct marketing business.[33] The other respondents either had no comment on the proposal or expressed only general views with no clear indication of stance on "support" or otherwise.

Sensitive Personal Data (Proposal 38)

12.5 20 respondents supported the proposal to afford a higher protection to sensitive personal data, against 10 respondents objecting. One respondent supporting the proposal pointed out that the exclusion of the proposal to protect sensitive personal data will make Hong Kong further lagging further behind its international counterparts[34]. Those respondents who have indicated their support also expressed views on which type of data should be classified as sensitive personal data. Based on the number of respondents indicating support for each data

30 Institute of Financial Planner of Hong Kong
31 Hong Kong Call Centre Association
32 Hong Kong Direct Marketing Association
33 Hong Kong Call Centre Association and Hong Kong Direct Marketing Association
34 Institute of Financial Planner of Hong Kong

type, a priority list could be drawn up as follows:-

Priority	Number of respondents indicating support	Type of data
(1)	11	- *data concerning health condition*
(2)	10 10	- *information on sex life* - *biometric data*
(3)	8	- *the commission or alleged commission of an offence and any proceedings relating to an offence alleged to have been committed*
(4)	5	- *personal data revealing racial or ethnic origin*
(5)	3 3	- *personal data revealing political opinions* - *personal data revealing religious or philosophical beliefs*
(6)	2	- *personal data revealing trade-union membership*

12.6 Further, one respondent[35] suggested that *"other intimate data that may be used in discriminatory decisions"* should also be included as sensitive personal data. Another respondent[36] suggested that for the benefit of vulnerable persons such as mentally incapacitated persons and children, data relating to mental health and medical records/treatments should also be classified as sensitive to afford them better protection. One other respondent[37] suggested to include location data as sensitive personal data.

35 Society for Community Organization.
36 Official Solicitor's Office
37 Professor Graham Greenleaf, Professor of Law & Information Systems, University of New South Wales, Sydney, Australia.

12.7 The other respondents either had no comment on the proposal or expressed only general views with no clear indication of stance on "support" or otherwise.

To empower the PCPD to Award Compensation to Aggrieved Data Subjects (Proposal 40)

12.8 10 respondents supported the proposal to empower the PCPD to award compensation to aggrieved data subjects, against 13 respondents objecting. The other respondents either had no comment on the proposal or expressed only general views with no clear indication of stance on "support" or otherwise.

12.9 It is worthy to note that one respondent pointed out clearly that the *Octopus* incident has indicated the weakness of the existing regulatory regime under the Ordinance and criticized the Commissioner's lack of power to award damages and assist complainants in civil actions[38].

To empower the PCPD to Impose Monetary Penalty on Serious Contravention of Data Protection Principles (Proposal 42)

12.10 13 respondents supported the proposal to empower the PCPD to impose monetary penalty on serious contravention of data protection principles, against 12 respondents objecting. One respondent supporting the proposal advocated that the PCPD as an independent regulatory body should be given more powers to impose penalties on serious contravention.[39] The other respondents either had no comment on the proposal or expressed only general views with no clear indication of stance on "support" or otherwise. For example, one respondent[40] expressed that each proposal has its pros and cons and there may be alternatives to achieve the same purpose, such as using the media to supervise and monitor.

---

38 Professor Greenleaf specifically referred to his article to be published in the BNA Privacy Law & Business, "*Octopus Scandal Exposes Hong Kong Privacy Deficiencies.*"

39 Institute of Financial Planner of Hong Kong.

40 The Internet Professional Association

On-line survey regarding Proposals 1, 38, 40 and 42

12.11 An on-line survey was launched by the PCPD from 8 December 2010 to 28 December 2010 to provide a convenient and easily accessible platform for the general public to express their views anonymously on the above four proposals. The results are set out below. They include also the written responses received through other miscellaneous channels from identifiable individuals and parties who fall outside the defined target group for the questionnaire survey mentioned in paragraphs 12.2-12.10 above.

12.12 A table summarizing the results of this survey is attached at the end of this document.

Setting up a territorial-wide "Do-not-call" Register for person-to-person telemarketing calls (related to Proposal 1)

12.13 1210 responses were received for this proposal. 464 respondents supported and 711 respondents objected to this proposal. The remaining 35 respondents elected to express no comment on the proposal.

Sensitive Personal Data (Proposal 38)

12.14 1208 responses were received for this proposal. 443 respondents supported and 701 respondents objected to this proposal. The remaining 64 respondents elected to express no comment on the proposal. Those respondents who have indicated their support also expressed views on which type of data should be classified as sensitive personal data and given a higher level of protection. Based on the percentage of these respondents indicating support for each data type, a priority list could be drawn up as follows: -

Priority	Percentage of respondents indicating support	Type of data
(1)	73%	- *information on sex life*
(2)	71%	- *data concerning health condition*
(3)	55%	- *biometric data*
(4)	50%	- *personal data revealing political opinions*
(5)	47%	- *the commission or alleged commission of an offence and any proceedings relating to an offence alleged to have been committed*
(6)	41% 41%	- *personal data revealing racial or ethnic origin* - *personal data revealing trade-union membership*
(7)	36%	- *personal data revealing religious or philosophical beliefs*

To empower the PCPD to Award Compensation to Aggrieved Data Subjects (Proposal 40)

12.15 1207 responses were received for this proposal. 319 respondents supported and 799 respondents objected to this proposal. The remaining 89 respondents elected to express no comment on the proposal.

To empower the PCPD to Impose Monetary Penalty on Serious Contravention of Data Protection Principles (Proposal 42)

12.16 1214 responses were received for this proposal. 389 respondents supported and 778 respondents objected to this proposal. The remaining 47 respondents elected to express no comment on the proposal.

Conclusions on surveys regarding Proposals 1, 38, 40 and 42

12.17 The Internet Protocol ("**IP**") addresses of the respondents to the on-line survey were recorded in the survey. From this record, several observations are noteworthy:- one call centre has submitted: (a) 292 responses to object the proposal to set up a territorial-wide "Do-not-call" Register for person-to-person telemarketing calls ("**related to Proposal 1**"); (b) 293 responses to object to the proposal to afford a higher protection to sensitive personal data ("**Proposal 38**"); (c) 292 responses to object to the proposal to empower the PCPD to award compensation to aggrieved data subjects ("**Proposal 40**"); and (d) 291 responses to object to the proposal to empower the PCPD to impose monetary penalty on serious contravention of Data Protection Principles ("**Proposal 42**").

12.18 If the responses from this call-centre were discounted, the results of the on-line survey do correspond with the results of the targeted survey mentioned above and the following conclusions could be drawn:-

(a) Majority view supports the setting up of a territorial-wide "Do-not-call" Register for person-to-person telemarketing calls, and affording greater protection for sensitive personal data. Over 50% of those in support consider that information concerning sex life and health condition, as well as biometric data, should be classified as sensitive personal data and given greater protection.

(b) The number of respondents objecting to the proposals to provide more sanctioning powers to PCPD is more or less the same as the number supporting the proposals.

Targeted Survey regarding Proposal 5

12.19 As regards Proposal 5 (the proposal to impose direct regulation on data processors and sub-contracting activities), it is mentioned in the Consultation Report that the IT sector generally objects to the proposal.

As part of its public engagement exercise, the PCPD attended various discussion sessions and forums organized by IT professional bodies, explained the proposal to them in greater details, and addressed their concerns and misconceptions. Subsequently, the PCPD sent out a questionnaire on 14 December 2010 to 10 IT professional bodies and Internet-related associations which had made submissions during the consultation exercise in 2009 and/or had approached the PCPD and expressed their concerns during the recent discussion sessions and forums.

12.20 Out of the 5 replies received, 4 supported Proposal 5 while the fifth respondent indicated that there were pros and cons under the proposal and hoped the matter would be further debated.

Concluding Remarks

12.21 Due to time and resource constraints, the PCPD accepts that there are limits in the surveys hence the results. However, taking into account the large number of respondents involved in such a short time and the fact that results from different surveys do tend to validate each other, they should serve as useful references for the public and the Administration to seriously consider resurrecting PCPD's proposals in the legislative amendment exercise.

Office of the Privacy Commissioner for Personal Data
31 December 2010

~~ END ~~

Online Survey Results

		Total	%	
Q1	Do-not-call Register - setting up of a territorial-wide Do-not-call register for person-to-person calls.			
	◆ Support the proposal	**464**	**38%**	
	◆ Object the proposal	**711**	**59%**	*
	◆ No comment on the proposal	**35**	**3%**	
	No. of respondents	***1210***		
Q2	Sensitive Personal Data - proposal to impose stringent regulation on sensitive personal data.			
	◆ Support the proposal	**443**	**37%**	
	◆ Object the proposal	**701**	**58%**	**
	◆ No comment on the proposal	**64**	**5%**	
	No. of respondents	***1208***		
Q3	Sensitive Personal Data - the following data should be classified as sensitive personal data.			
	◆ personal data revealing racial or ethnic origin	**238**	**41%**	
	◆ personal data revealing political opinions	**288**	**50%**	
	◆ personal data revealing religious or philosophical beliefs	**207**	**36%**	
	◆ personal data revealing trade-union membership	**237**	**41%**	
	◆ data concerning health condition	**405**	**71%**	
	◆ information on sex life	**419**	**73%**	
	◆ the commission or alleged commission of an offence and any proceedings relating to an offence alleged to have been committed	**272**	**47%**	
	◆ biometric data	**317**	**55%**	
	◆ Other	**58**	**10%**	
	No. of respondents	***574***		
Q4	PCPD to award compensation to aggrieved data subjects and to encourage settlement by reconciliation.			
	◆ Support the proposal	**319**	**26%**	
	◆ Object the proposal	**799**	**66%**	***
	◆ No comment on the proposal	**89**	**8%**	
	No. of respondents	***1207***		
Q5	Impose Monetary Penalty on Serious Contravention of Data Protection Principles.			
	◆ Support the proposal	**389**	**32%**	
	◆ Object the proposal	**778**	**64%**	****
	◆ No comment on the proposal	**47**	**4%**	
	No. of respondents	***1214***		

*** includes 292 responses submitted by a call centre**
**** includes 293 responses submitted by a call centre**
***** includes 292 responses submitted by a call centre**
****** includes 291 responses submitted by a call centre**