PCPD's Information Paper

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. Purpose

1. More than a decade has passed since the Personal Data (Privacy) Ordinance (Cap.486) ("the Ordinance") came into force on 20 December 1996. The rapid technological and electronic trade and commerce developments that are taking place and the exponential rate with which it continues to progress give rise to global personal data privacy concern.

2. Overseas governments and privacy regulators see a pressing need for reviewing and reforming the privacy law in order to safeguard the personal data privacy interests of the individuals. Australia, Canada, New Zealand and the United Kingdom all embark actively on the review of their laws. By way of illustration, Australia's consultation exercise is the biggest of its kind in recent years. The report contains 2693 pages. The global trend is to aspire for a higher level of personal data privacy protection and stronger sanction and legislation to properly address the privacy impact brought about by technological advancements.

3. Personal data privacy has been an evolving concept in human rights and electronic trade and commerce responding to rapid changes and development brought about by modern technology. The Privacy Commissioner acknowledges the core value of balancing the personal data privacy right with other rights and social interest in maintaining a harmonious society. With a decade of regulatory experience gained in the discharge of his Office's regulatory duties and without losing sight to the macro international privacy perspectives that are taking shape, the Commissioner finds it appropriate and timely to conduct a comprehensive review of the Ordinance. With these objectives in mind, an internal Ordinance Review Working Group was set up in June 2006 to assess the adequacy of the protection rendered to personal data privacy by the Ordinance.

4. In the course of his review of the Ordinance, the Commissioner has taken 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 the Commissioner gained in the course of discharging his functions and powers;

(d) the difficulties encountered 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.

5. In December 2007, the Privacy Commissioner for Personal Data (PCPD) provided the Constitutional and Mainland Affairs Bureau ("the CMAB") with a comprehensive package of over 50 amendment proposals.

6. Having considered and discussed with the PCPD the proposals, the CMAB released the Consultation Document on Review of the Personal Data (Privacy) Ordinance on 28 August 2009 ("the Consultation Paper"). This Information Paper provides the public with additional materials to consider before making submissions to the consultation. Members of the public are encouraged to read this Information Paper in conjunction with the Consultation Paper.

7. To enable the public to have a holistic view of the Ordinance Review Exercise undertaken by the PCPD since 2006, proposals made by the PCPD to the CMAB as well as relevant issues of privacy concern are attached at the Annex of this Information Paper.

8. Some of the proposed amendments will have significant impact on various sectors of the community. The Commissioner considers that it is imperative that the Government should seriously consider all responses from the public. He therefore strongly urge members of the public to make their submissions to the CMAB on or before 30 November 2009.

Office of the Privacy Commissioner for Personal Data
9 September 2009

II. Information and Materials on Amendment Proposals

Proposal No. 1 : Sensitive Personal Data

Scope of sensitive personal data

2.1 Paragraph 3.02 of Chapter 3 of the Consultation Paper (at p.10) refers to various international practices and standards on the regulation of sensitive personal data. The following table seeks to elaborate on such international practices and standards.

International Practices or Standards	Categories of personal data which processing is prohibited except as prescribed
European Parliament's Directive 95/46/EC[1]	➢ Processing of special categories of data: "Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life." (Article 8(1)) ➢ "Processing of data relating to offence, criminal convictions or security measures may be carried out only under the control of official authority or if suitable specific safeguards are provided under national law…" (Article 8(5)) ➢ "Member States may provide that data relating to administrative sanctions or judgment in civil cases shall also be processed under the control of official authority." (Article 8(5))
UK Data Protection Act 1998[2]	➢ Sensitive personal data is defined as "personal data consisting of information as to- (a) the racial or ethnic origin of the data

[1] The EU Directive on "*The protection of individuals with regard to the processing of personal data and on the free movement of such data*" was issued on 24 October 1995.

[2] Available at http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1

	subject; (b) his political opinions; (c) his religious beliefs or other beliefs of a similar nature; (d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992); (e) his physical or mental health or condition; (f) his sexual life; (g) the commission or alleged commission by him of any offence; or (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings" (section 2)
Privacy Act 1988, Australia[3]	➢ "Sensitive information" is defined as: "(a) information or an opinion about an individual's— (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual preferences or practices; or (ix) criminal records; that is also personal information; or (b) health information about an individual; or (c) genetic information about an

[3] Available at http://www.comlaw.gov.au/ComLaw/legislation/actcompilation1.nsf/framelodgmentattachments/9D7FF2906FD6A6D4CA2575C50002F679

	individual that is not otherwise health information." (section 6)
Australian Law Reform Commission ("ALRC") - Discussion Paper 72 - Review of Australian Privacy Law[4]	➢ The ALRC proposes the definition of "sensitive information" in Australian Privacy Act should also include:- (a) biometric information collected for the purpose of automated biometric authentication or identification; and (b) biometric template information. ➢ The ALRC also proposes that the phrase "sexual preferences and practices" currently used in the definition of "sensitive information" should be changed to "sexual orientation and practices".

2.2 Processing of special categories of data without the consent of the data subjects is prohibited except under special circumstances. Such special circumstances commonly found in privacy legislations include:-

(1) necessary for the purpose of carrying out obligations and specific rights of the data user/controller in the field of employment law;

(2) necessary to protect vital interests of data subject or of another person where data subject is physically or legally incapable of giving his consent;

(3) necessary for establishment, exercise or defence of a legal claim;

(4) the relevant data are manifestly made public by the data subject;

(5) carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit seeking body with a political, philosophical, religious or trade-union aim and on the condition that the processing relates solely to the members of the body or to

[4] Available at http://www.austlii.edu.au/au/other/alrc/publications/dp/72/DP72.pdf

persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects;

(6) necessary for medical purpose and where the data are processed by a health professional subject to duty of confidentiality; and

(7) where the collection is required by law.

2.3 The UK Privacy Act 1998 provides an additional exception to processing of personal data relating to racial or ethnic origin necessary for equality of opportunity and treatment between different racial or ethnic origins. Another exception is where the processing is necessary for administration of justice or for exercise of function conferred by an enactment or for exercise of function of the Crown.

2.4 The Australian Privacy Act 1988 further provides an exception to the collection of health information necessary for research or analysis of statistics relevant to public health or safety or management of health services.

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

Proposed obligations on data users

3.1 At present, section 4 of the Ordinance prohibits a data user from doing an act or engaging in a practice that contravenes a data protection principle unless the act or practice is required or permitted under the Ordinance. Data Protection Principle 4 which aims to safeguard the security of personal data provides:-

> *"All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure or other use having particular regard to-*
> *(a) the kind of data and the harm that could result if any of those things should occur;*
> *(b) the physical location where the data are stored;*
> *(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data are stored;*
> *(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data, and*
> *(e) any measures taken for ensuring the secure transmission of the data."*

3.2 It is not uncommon for local organizations to outsource their work process involving personal data to contractors. If the contractors fail to safeguard the security of the personal data obtained from the organizations, such as causing leakage of the data, the organizations will be liable as the contractors' principal by virtue of section 65(2) of the Ordinance. It is because pursuant to the provision, any act done by an agent (i.e. the contractor) with the authority of principal (i.e. the organization) will be treated as done by the principal (i.e. the organization).

3.3 It is now proposed in paragraphs 4.09 and 4.10 of Chapter 4 of the Consultation Paper (at p.19-20) that specific obligations should be imposed on the data users by requiring them to take specific security measures when contracting out the processing of personal data to third parties. The specific measures would be to require the data users to use contractual or other means to ensure that their data processors will provide security protection to the

personal data at a level comparable to their own obligations under the Ordinance. The requirement is to be applied to contractors and their sub-contractors as well, no matter whether they are within Hong Kong or offshore.

3.4 The PCPD expects a data user, in order to comply with the proposed specific obligation, to select a reputable contractor that offers guarantees on its ability to ensure the security of the personal data. The terms of the service agreement shall also provide the following:-

(a) prohibiting the contractor to use or disclose the personal data for a purpose other than the purpose for which the outsourced contractor is assigned to carry out;

(b) security measures required to be taken by the contractor to protect the personal data given to them and obliging the contractor to protect the personal data by complying with the data protection principles of the Ordinance;

(c) requiring a timely return or destruction of the personal data when they are no longer required for the purpose for which the contractor is assigned to carry out;

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

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

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

3.5 Organizations usually enter into formal contractual agreements with the contractors for processing personal data. Inclusion of specific contractual terms will not cause any additional burden on organizations. For transfer of personal data outside Hong Kong, there is also a statutory requirement under section 33(2)(f) (though not yet effective) on a data user to take all reasonable precautions and to exercise all due diligence to ensure that the personal data will not be collected, held, processed or used in a place outside Hong Kong in any manner which, if that place were Hong Kong, would be a contravention of a requirement under the Ordinance.

Proposed obligations on data processors

3.6 Paragraph 4.08 of Chapter 4 of the Consultation Paper (at p.19) defines a "data processor" as "any party, other than an employee, who holds, processes or uses personal data solely on behalf of a data user, and does not hold, process or use those data for any of his own purposes". Some common examples are: processing agents (e.g. where personal data are entrusted for carrying out data entry and pay-roll calculation, etc); IT service providers (e.g. where personal data are entrusted to them for carrying out program testing); document shredding service providers, Internet service providers ("ISPs") (e.g. when they are providing a platform for communication).

3.7 Although data processors do not hold, process or use personal data for their own purposes, it is through their business that personal data are being collected, held, processed or transferred.

3.8 The recent spate of the incidents of loss or leakage of personal data stored in electronic form, in particular, portable electronic device by contractors of the data users reflect that specific obligations should be imposed on persons who are entrusted to process data.

ISPs and web-based service providers

3.9 The ISPs and webmail service providers are classes of persons serving as conduit pipe for personal data traffic. They provide platforms where data are stored and hoarded, which will expose personal data to higher security risk.

3.10 ISPs and web-based service providers process huge amount of information in the course of their businesses, and it is not unusual that the information may contain personal data. They are in any case expected not to misuse the personal data they obtained or to retain the information they process indefinitely. Moreover, they are expected to ensure that their systems are secure and safe to use.

3.11 The mere fact that they cannot pinpoint on each occasion whether they are processing personal data in carrying out subscribers' or users' instructions should not excuse them from the obligation to protect personal data. In fact, this proposal does not require ISPs and web-based service providers to examine each piece of information they process in order to find out whether it contains personal data, what kind of personal data they are, and what appropriate

measures should be taken to protect them. They may simply treat each piece of information they obtained in the process as "personal data" and safeguard the data security as well as against any misuse or excessive retention.

3.12 In considering whether IP addresses are personal data, the EU Working Party 29 holds the view that "*…unless the Internet Service Provider is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified, it will have to treat all ISP information personal data, to be on the safe side…*" Similarly, as prudent service providers, they may treat the information they process as containing personal data and comply with DPP2(2), 3 and 4.

Imposing obligations on both the data users and the data processors in order to afford adequate data protection at all levels

3.13 The proposal of imposing separate obligations on data processors to comply with DPP2(2), 3 and 4 under paragraph 4.14 in Chapter 4 of the Consultation Paper (p.21) is to ensure that they will exercise the same level of diligence as is required of the data users in ensuring security of their systems, making sure personal data are properly used and not kept longer than is necessary. The proposed requirement that data users have to use contractual or other means to require data processors to provide a comparable level of security protection spells out a distinct obligation for data protection if they transfer personal data to data processors. The proposed obligations serve to protect personal data at different levels. The obligations on data processors would not become unnecessary if a higher standard of obligations is imposed on data users or vice versa.

Proposal No. 3 : Personal Data Security Breach Notification

4.1 In responding to the spate of data leakage incidents, the Government introduced a notification mechanism for personal data leakage incidents. Bureaux and departments are required to report data leakage incidents to the PCPD as soon as possible and notify affected individuals as far as practicable.

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

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

4.4 For better understanding of how it operates, below is a compliance check case which was initiated after receiving a data breach notification :

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

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

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

4.4.4 Having considered the written undertaking and the remedial actions taken by the company, the PCPD decided not to take further action.

4.5 Government departments and public bodies collect huge amount of personal data of citizens. Imposing notification requirement on them would not be unduly burdensome as they have already implemented a voluntary notification system. Members of the public may comment on whether it is desirable to make it mandatory for Government departments and public bodies to give security breach notification.

Proposal No. 4 : Granting Prosecution Power to the PCPD

At present, the PCPD refers cases to the Police to carry out criminal investigation and prosecution under the Ordinance.

5.2 Apart from the reasons stated in paragraph 5.03 of Chapter 5 of the Consultation Paper (at p.31) justifying the proposal, conferring power on the PCPD to institute prosecution proceedings will avoid public criticism that there exists a conflict of interest in case where the Police or a government department is the relevant data user involving in a possible infringement of the Ordinance. It is necessary to maintain impartiality in the eyes of the public.

Proposal No. 6 : Award Compensation to Aggrieved Data Subjects

6.1 In the wake of the data leakage of 20,000 complainants' personal data by the Independent Police Complaints Council in 2006, there have been concerns and criticisms on the PCPD's lack of power to award compensation after making a finding that a data user had infringed the requirement of the Ordinance.

6.2 At present, an aggrieved person who suffers damage or loss by reason of a contravention of a requirement of the Ordinance is required to take civil action by himself to seek compensation from the relevant data user. To take out a court action is generally timely and costly and the individual has to deal with the matter on his own unless he has sufficient means to engage a lawyer or is otherwise entitled to obtain legal aid.

6.3 Over the years, the PCPD notices that civil action under section 66 of the Ordinance is rarely invoked. There has been no reported case found where compensation was awarded. One possible reason is due to the lengthy and costly litigation process.

6.4 The proposal to confer power on the PCPD to award compensation after conclusion of an investigation will strengthen the protection afforded to aggrieved individuals. An equivalent provision modeling on section 52 of the Australian Privacy Act will provide a quick and effective mechanism to redress any infringement of the requirement of the Ordinance. The amount of compensation may be settled through mediation to be conducted by the PCPD.

6.5 If the proposal is adopted in the Ordinance, an aggrieved individual may decide whether to institute a court action or to seek compensation through this proposed procedure.

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

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

7.1 Certain activities infringing personal data privacy have been singled out as offences under the current legislation: they are the non-compliance with a data access/correction request (sections 19 and 23), failure to erase personal data no longer required (section 26), carrying out matching procedures other than in accordance with prescribed conditions (section 30), and direct marketing made to individual who has opted-out from receiving the same (section 34). Apart from the requirements under sections 19, 23 and 26 which are also covered by DPP6 and DPP2(2), there is no general provision making non-compliance with a data protection principle *per se* an offence.

7.2 The situation is in line with international jurisprudence on privacy legislation. It has been recognized that the effective means of ensuring the proper behaviour and attitude towards protection of personal data privacy is by regulation and education rather than criminal sanction.

7.3 Making contravention of data protection principles *per se* an offence will have a significant impact on civil liberty given that an inadvertent act or omission on the part of a data user might turn him into a criminal. Strong grounds of justification are needed for such a legislative proposal. Factors that are relevant for consideration will include: (a) whether the act or practice in question needs to be controlled by imposing criminal sanction; and (b) whether the element of culpable intent is present.

A selective Approach

7.4 A selective approach is preferred whereby particular acts or practices are singled out as offences having regard to the severity of such contravening acts or practices. To deter acts such as downloading or disseminating of personal data leaked on the Internet, the PCPD proposes to create a new offence modeling on section 55 of the UK Data Protection Act. Further details of the offence are provided at paragraphs 8.1 to 8.6 below and the PCPD's Proposal No. 41 in the Annex.

7.5 Another aspect of the selective approach is to introduce a monetary penalty for failure to comply with the data protection principles but limited to breaches that are avoidable and that give rise to a serious data protection risk.

It would address behaviour that reveals either a wilful disregard for the requirements of the Ordinance or a grossly negligent approach to complying with the requirements. More details about the monetary penalty are provided under the PCPD's Proposal 52 in the Annex.

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

8.1 Section 55 of the UK Data Protection Act makes it an offence for any person who knowingly or recklessly, without the consent of the data controller, obtains or discloses personal data or procure such disclosure unless justifiable grounds exist, e.g. for prevention or detection of crime, or as required by or authorized by law. Section 55(4) to (6) of the Act prohibits the selling or offering to sell the personal data so obtained by making it an offence.

Objective is not to penalize unintentional or accidental leakage of personal data by data user

8.2 It is mentioned in paragraph 6.09 of Chapter 6 of the Consultation Paper (at p.40) that the objective of this proposal is not to penalize the data user who leaked the data but to protect data subjects whose personal data were leaked and to deter irresponsible acts of those who obtain or disclose such leaked data without consent. For data users responsible for the leakage of personal data, they will be sanctioned under the existing provisions of the Ordinance as well as proposed new provision of imposing monetary penalty. It should be noted while the PCPD has no intention to turn data users responsible for accidental leakage into criminals, for cases where the contravention was serious and which resulted in substantial risk of harm to the data subjects, it is proposed that the PCPD may impose monetary penalty on those occasions.

The proposal will not interfere normal and innocuous browsing activities of web-users

8.3 Paragraph 6.10 of Chapter 6 of the Consultation Paper (at p.40) raises the concern that the proposed offence may interfere with the normal and innocuous browsing activities of web-users.

8.4 The PCPD does not agree. Taking the situation in the UK as an example, the provision has taken effect for more than 8 years, the PCPD does not aware of any public concerns that the offence affects ordinary Internet users. The person downloading personal data from the Internet has *"reasonable belief"* defence that he had a lawful right to obtain or that the user would have consented to the obtaining. Only those who act *"knowingly or recklessly"* will be affected by the offence. It is also noted that the proposed new offence

should not affect the continued operation of Part VIII exemption of the Ordinance to provide valid grounds for exemption to be invoked in appropriate cases. Section 52 of the Ordinance provides an exemption from the provisions of the DPPs where personal data are held by an individual and concerned only with the management of his personal, family or household affairs or so held only for recreational purposes.

Restricting the offence to disclosure of data so obtained for profits or malicious purpose will not be able to mend the current loophole

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

8.6 Members of the public are encouraged to consider section 55 of the Data Protection Act and section 77 and 78 of the Criminal Justice and Immigration Act (which recently made certain amendments to section 55 of the Data Protection Act by providing a new defence on journalistic activities). The relevant provisions are attached to the PCPD's Proposal no. 41 in the Annex.

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

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

9.1 Paragraphs 6.15 and 6.24 of Chapter 6 of the Consultation Paper (at p.42 and 44) state that there does not appear to be a strong case to introduce the above offences as the PCPD has not come across any such case since the enactment of the Ordinance.

9.2 The PCPD believes that prevention is better than cure. It should be noted that these two proposals are part and parcel of the PCPD's package of proposals to strengthen the enforcement powers and to deter non-compliance with the requirements of the Ordinance.

9.3 At present, the enforcement power of the Ordinance is comparatively weak in that the Commissioner's power to issue an enforcement notice is very much restricted by section 50 of the Ordinance. This may account for the reason why the PCPD has not come across repeated contravention of a DPP on the same facts shortly after compliance with an enforcement notice issued on the relevant data user. Proposal has been made to amend section 50 by granting wider discretionary power on the PCPD to issue enforcement notices. According to the experience of the PCPD, it is not rare that different complainants complain against the same data user at different times for contravention of the Ordinance on the same or similar facts.

9.4 The culpability of repeated offenders is more rampant than a first-time offender and it is not uncommon for local legislations to impose heavier penalty on repeated offenders.

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

10.1 The PCPD has from time to time referred cases involving suspected contravention of section 34 of the Ordinance (direct marketing provisions) to the Police for criminal investigation and prosecution. At present, an offender who contravenes section 34 of the Ordinance is liable to a maximum penalty of HK$10,000 under section 64(10) of the Ordinance.

The maximum penalty of HK$10,000 is hardly a deterrent

10.2 Below are some of the conviction cases where the offenders had failed to observe the complainants' opt-out requests by repeatedly using the complainants' personal data for direct marketing purpose.

Case 1

In January 2007, a telecommunications company was convicted of breaching section 34(1)(ii) of the Ordinance. The case was heard at Kwun Tong Magistrates' Courts where four summonses were laid against the company for contravening section 34 (ii) of the Ordinance, which requires data users to cease further contact with the individual if he chooses to opt-out.

The company began contacting the complainant by phone to promote its IDD services in July 2005. The complainant asked the company several times to stop calling him for direct marketing purposes. Nonetheless, the company continued to call him on a number of occasions for direct marketing purposes despite his opt-out requests. In February 2006, the complainant lodged a complaint with the PCPD.

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

The company pleaded guilty to all summonses. The magistrate

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

Case 2

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

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

Having learned that the complainant had made a complaint to the PCPD, the company sent a letter of apology to him. The company also agreed to process the complainant's opt-out request by removing his data from their mailing list. Notwithstanding these, the complainant still received marketing mails from the company on 15 January and 3 February 2007 respectively.

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

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

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

11.1 The Consultation Paper has highlighted the current restrictions under section 50 of the Ordinance to issue an enforcement notice. Paragraph 39 of Annex 1 of the Consultation Paper (at p.60-61) proposes to enhance the effectiveness of the Ordinance by allowing discretion for the PCPD to serve an enforcement notice having due regard to the following circumstances. They are:-

(a) whether the act of contravention is continuing;
(b) whether the contravention will continue or be repeated;
(c) whether the contravention has caused or is likely to cause damage or distress to the data subject.

11.2 It should be noted that the circumstances under (a), (b) and (c) are already provided in section 50(1)(a), 50(1)(b) and 50(2). While rewriting the provisions would certainly give more flexibility for PCPD to serve an enforcement notice, the PCPD indeed proposes an additional paragraph (d) *"such matters as the Commissioner may think fit to consider"* for the Administration's consideration.

11.3 This paragraph (d) will enable the PCPD to consider also other relevant circumstances in the specific cases. In deciding whether to issue an enforcement notice, the PCPD wishes to be able to consider, amongst other things, the following:-

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

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

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

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

(e) the conduct of the data user during the incident in question, after being notified of the subject matter of the complaint (whether by the complainant, the media, PCPD, other regulators or other sources), and during the course of the investigation (whether co-operative, whether providing misleading

information, whether remorseful, etc.);

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

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

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

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

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

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

Case 1

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

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

complainants personal data; and (iv) making an apology to the complainants.

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

Case 2

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

Case 3

The complainant alleged that a company had collected a copy of her Hong Kong identity card prior to the granting of a job interview. Upon intervention by this Office, the company confirmed that they had destroyed all HKID copies of job applicants previously obtained, and undertook that they would not collect the HKID copies of job applicants unless and until the individual had accepted an offer of employment. In light of the above remedial actions taken by the company, the PCPD had not served an enforcement notice since no evidence of likelihood of repetition of the contravention could be found.

Case 4

The complainant had a dispute with a travel agent over the amount to be charged on cancellation of an air flight booking. The complainant later discovered that the travel agent had, without his consent, used the personal data collected during the booking transaction for lodging a complaint against him to his employer thereby disclosing the details of the dispute. Upon investigation by the PCPD, the travel agent confirmed that (i) she would not use

the complainant's personal data for any purpose other than air flight booking and related matters; (ii) the information collected during booking transaction had formed part of internal document retained by employer of the travel agent and she had not retained a copy of the complainant's personal data. In view of the aforesaid, the PCPD did not issue an enforcement notice as no evidence of likelihood of repetition of contravention was found.

Case 5

The complainant opened an account with a ticket company for purchasing cinema and concerts tickets online by credit card. During online registration, the complainant chose not to receive direct email newsletter but he still received 3 marketing emails from the company at his email address. Subsequently, the company took remedial actions by (i) removing complainant's email address from the mailing list (ii) amending the opt-out statement; and (iii) conducting manual check of mailing list to ensure no inclusion of subscribers who had opted out. In view of the remedial actions taken, there was no evidence of likelihood of repetition of the contravention by the company. Thus, no enforcement notice could be served on the company by the PCPD.

Case 6

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

Case 7

The complainant ceased to be a customer of a telecommunications company. Later, he discovered that the telecommunications company debited his credit card for a service fee. As the complainant had never provided his credit card number to the company, he lodged a complaint with the PCPD. Our investigation revealed that the telecommunications company had made a clerical mistake by wrongly debiting the complainant's credit card account for a fee incurred by another customer. The telecommunications company stated that they had a policy in place requiring their staff to verify the accuracy of customers' personal data and in order to avoid recurrence of similar incident in future, they had advised their staff to double-check the credit card account number before transferring the same to the bank. In view of the remedial action taken by the company, the PCPD opined that the contravention was not likely to be repeated and therefore no enforcement notice was issued.

Case 8

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

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

11.7 The PCPD is not aware of any of its overseas counterparts being restricted by their respective laws the discretion to issue enforcement notices in such a way as provided for under the Ordinance. For example, the UK Data

Protection Act 1998 provides under section 40 the power of the UK Information Commissioner to issue enforcement notices as follows:-

> *"40 (1) If the Commissioner is satisfied that a data controller has contravened or is contravening any of the data protection principles, the Commissioner may serve him with a notice (in this Act referred to as "an enforcement notice") requiring him, for complying with the principle or principles in question, to do either or both of the following:-*
>
> *(a) to take within such time as may be specified in the notice, or to refrain from taking after such time as may be so specified, such steps as are so specified, or*
>
> *(b) to refrain from processing any personal data, or any personal data of a description specified in the notice, or to refrain from processing them for a purpose so specified or in a manner so specified, after such time as may be so specified.*
>
> *(2) In deciding whether to serve an enforcement notice, the Commissioner shall consider whether the contravention has caused or is likely to cause any person damage or distress.*

11.8 While the legislative intent behind the introduction of the conditions under section 50(1)(a) and (b) may be more on an educational value due to the protection of personal data privacy being a concept new to the community in the early days when the Ordinance was enacted, it is timely to make a change after 12 years of its coming into operation. From the perspective of better personal data privacy protection and for the purpose of controlling the improper act or practice done or engaged in by the data user, the issuance of an enforcement notice has deterrence effect upon the infringers given the offence sanction imposed under section 64(7) for breach of an enforcement notice.

11.9 The catch-all factor under paragraph (d) of the PCPD's proposal will not confer on the PCPD an unfettered discretion to issue enforcement notices. It should be noted the Commissioner's exercise of his discretion to issue an enforcement notice is subject to challenge. Pursuant to section 50(7), the relevant data user to whom the enforcement notice is served may appeal to the Administrative Appeals Board ("AAB"). After all, the purpose of issuing an enforcement notice on a data user is to impose obligation on the data user to take steps to remedy the contravention. A data user who is remorseful about the act done or practice engaged will be more than willing to comply with the terms of the enforcement notice.

11.10 The proposed amendments will confer a more reasonable degree of flexibility to the PCPD in the exercise of its enforcement powers which is desirable for attaining the objective of the Ordinance.

Proposal No. 23 : Additional Grounds for Refusing to Investigate

Where a complaint relates to an action for which the complainant has a remedy in any court or tribunal

12.1 In paragraph 46 of Annex 1 of the Consultation Paper (at p.63), the Administration expresses their reservations in supporting as a ground for the PCPD to refuse to investigate *"if a complaint relates to an action for which the complainant has a remedy in any court or tribunal"*. It is suggested that an aggrieved party will be deprived of an alternative for redress if the PCPD is to refuse investigation on such ground.

12.2 The rationale for this proposal by the PCPD can be found in PCPD's Proposal No. 12 in the Annex.

12.3 In making the proposal, the PCPD has made reference to section 10(1)(e)(ii) of the Ombudsman Ordinance which provides as follows:-

> "*10(1) Notwithstanding the generality of the powers conferred on the Ombudsman by this Ordinance, the Ombudsman shall not undertake or continue an investigation into a complaint-*
>
> *(e) if the complaint relates to any action in respect of which the complainant has or had-*
>
> *(i) ….*
>
> *(ii) a remedy by way of proceedings in a court, other than by way of judicial review, or in any tribunal constituted by or under any Ordinance,*
>
> *unless the Ombudsman is satisfied that in the particular circumstances it is not reasonable to expect the complainant to resort or to have resorted to that right or remedy.*

12.4 In particular, the PCPD would be unlikely to intervene where the proper forum for resolving the dispute in question lies not with the PCPD but with other redress bodies. In assessing the gravity of the matter and the sanction imposed under other laws or ordinances for effective remedy and protection of the rights infringed, the PCPD may not be an appropriate body to deal with those cases.

12.5 For example, in AAB Appeal No.22/2000, an ex-employee sought to

correct the remarks and comments made by his ex-employer in the letter of dismissal by way of making a data correction request under section 22 of the Ordinance. The AAB took the view that in a notice of termination, personal data dealing with the employee's job performance was inherently contentious and it was unlikely that the dismissed employee would share the employer's point of view. The AAB opined that the proper venue to resolve such dispute lies with the Labour Tribunal. In the past decade, the PCPD has received many such highly contentious complaints which should be properly resolved by other redress bodies.

12.6 The PCPD's proposal contains a saving clause "*where in the particular circumstances it is not reasonable to expect the complainant to resort or to have resorted to the right or remedy in court or tribunal or to lodge a complaint with a regulatory body… or law enforcement agencies"*. The saving clause will provide sufficient safeguard to an aggrieved party.

Where the primary cause of the complaint is not related to personal data privacy

12.7 Paragraph 47 of Annex 1 of the Consultation Paper (at p.63) states that this ground of refusal could be perceived as taking away the right of a data subject to have his complaint, which relates to personal data privacy, from being investigated. This is not the case. A comprehensive study of the following complaint cases received by the PCPD will help to clarify the reasons why such a proposal was made.

> ***Case 1***
>
> *The daughter of the complainant posted a notice with the headline "The present chairman xxx arrogates all powers to himself" in the public area of the building.*
>
> *In response to the notice, the chairman of the Incorporated Owners ("IO") xxx issued a memo, which contained the name of the complainant. In this connection, the complainant complained that the chairman of the IO had disclosed his personal data, and the IO "criticized owners with big-character poster of the Cultural Revolution".*
>
> *The PCPD opines that from the nature of the incident (scolding and libel), the complaint was not related to personal data privacy.*

Case 2

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

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

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

Case 3

The complainant was a customer of a telecommunication company.

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

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

Case 4

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

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

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

Case 5

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

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

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

Enquiry with the manufacturer revealed that it had recorded the correct date of birth of the complainant. The incident was caused by the setting of its system. It was not related to personal data privacy.

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

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

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

12.10 The PCPD agrees with the observation made by the AAB. Very often, it is found that some complainants have utilized the complaint channel provided under the Ordinance for personal feud rather than being motivated by a genuine concern for protection of one's personal data privacy. The PCPD

considers that the complaint channel under the Ordinance should not be used as a forum for the pursuit of personal dispute not related to personal data privacy.

A.2 - Internet Protocol Address as Personal Data

13.1 The existing three-limb definition of "personal data" gives general guiding principles on what constitutes "personal data" without singling out any particular kind of data to be so classified. The definition is of pretty straight forward application save for the concept of "indirect" identification and relevancy. In order that the definition is of meaningful application, the PCPD is mindful to take into account what is "reasonably practicable" for the data user to ascertain the identity of the individual, e.g. by reference to other information that is readily obtainable by it.

13.2 It was not until the Yahoo's case where heated debates were raised on whether IP address should be viewed as "personal data", as it can give useful hints for tracing the identity of the actual user of the computer. In the Yahoo's case, the PCPD took the view that an IP address *per se* does not meet the definition of "personal data". However, "personal data" can include an IP address when combined with, for example, identifying particulars of an individual.

13.3 The Yahoo's case went before the AAB. The Appellant relied on *Cinepoly Records Co Ltd and others v Hong Kong Broadband Network Ltd and others* [2006] 1 HKLRD 255 to illustrate how an IP address might be used to track down the identity of a certain data subject. Having considered the evidence before it, the AAB dismissed the appeal and decided that on the facts of the case, the IP log-in information provided by Beijing Yahoo! even when coupled with other information disclosed, did not constitute "personal data " as defined under the Ordinance. The AAB did not specifically rule on whether an IP address *per se* is "personal data" under the Ordinance because the Appellant had decided to drop the argument.

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

13.5 In view of the public concern, it is necessary to go through the consultation process to ascertain whether the community is in favour of affording IP address the same protection of "personal data" under the Ordinance.

13.6 To enable the general public to consider the issue, the PCPD sets out below the pros and cons for deeming IP address as personal data.

Pros

- it gives certainty on its classification;

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

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

Cons

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

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

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

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

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

LAN owner/operator), identifying an Ipv6 host device may be possible on most of the data recipient’s sides.

B.1 - Public Interest Determination

14.1 Unlike data privacy legislation in some overseas jurisdictions, there is no exemption in Ordinance for "public interest".

United Kingdom

14.2 In UK, public interest is expressly provided in Data Protection Act 1998 as a factor for considering whether personal data are fairly handled. For instance, Schedule 2 of the Act provides that it is relevant for consideration that "*the processing* (of personal data) *is necessary for the exercise of…functions of a public nature exercised in the public interest by any person*". Similarly, in Schedule 4, it is provided that the eighth principle does not apply if "*the transfer* (of personal data) *is necessary for reasons of substantial public interest*".

14.3 "Public interest" is even recognized as a defence to criminal offences in unlawful obtaining of personal data and unlawful requesting of employment related records (see s.55(2)(d) and s.56(3)(b) of the Act).

New Zealand

14.4 In New Zealand, the Privacy Commissioner may grant authorization to collection, use, or disclosure of personal information that was otherwise in breach of the information privacy principles, if public interest substantially outweighs the interference with the privacy that could result (see s.54 of New Zealand Privacy Act 1993).

Australia

14.5 Like New Zealand, the Privacy Commissioner in Australia is empowered to make determination to exempt an otherwise infringing act (see: Part VI of Privacy Act 1988), after balancing the public interest in doing the act and that in adhering to the information privacy principle (or National Privacy Principle as the case may be). To cater for situations which call for urgent determination, the Commissioner is also empowered to issue a Temporary Public Interest Determination.

Necessity of a public interest exemption in the Ordinance

14.6 At the meeting of the Panel on Constitutional Affair of Legislative Council held on 15 December 2008, LegCo members queried on the deficiency of the Ordinance in enabling disclosure of personal data in the public interest.

This proposal serves as a possible solution for discussion in the public consultation exercise.

14.7 To assist the public in examining the proposal, some examples are provided below showing the problems faced by data users when the PCPD does not have a power to make public interest determination.

Example 1

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

Example 2

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

14.8 As it is impracticable to provide an exemption to all possible situations

where in the consideration of public interest the provisions of the DPPs should not be applied, the addition of a general public interest exemption would serve to cover all necessary cases. Having said that, it is conceived that "public interest" being a generic term as it is may be subject to abusive use. Alternatively, it is worth considering the cloning (with necessary modification) of the Public Interest Determination ("PID") mechanism from the Australian Privacy Act 1988. PID is operated on *ad hoc* basis upon application made by the concerned data user. The Commissioner will balance the public interest in permitting the act or practice with the privacy protection in enforcing the legislation. Then, the Commissioner may determine whether to allow the act or practice to be conducted or engaged in within a given time period (with conditions imposed, if appropriate), or to dismiss the application.

14.9 Another practical advantage of adopting PID over the addition of a general public interest exemption is that the Commissioner may impose controls on the act or practice to be conducted or engaged in so as to tailor-make the case to maintain public interest at the minimal scarification of personal data privacy. For instance, a decision to allow the disclosure of personal data may saddle the data user with a prohibition in disclosing certain kind of data, such as identity card number or name.

14.10 The proposal will provide a direct solution to enable a data user to release the relevant data in the public interest without contravening DPP3 where the circumstances require a timely disclosure. Instead of making a blanket public interest exemption, the proposed scheme represents a gradual process whereby the Commissioner is charged with the function to determine in each and particular case whether there is justifiable overriding public interest that outweighs the data privacy right of individuals.

Annex

Amendment Proposals made by PCPD's Internal Ordinance Review Working Group

This Annex incorporates all the proposals and relevant issues of privacy concerns prepared by the PCPD's internal Ordinance Review Working Group since 2006.

III. Annex – PCPD's proposals to amend the Personal Data (Privacy) Ordinance

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 1

To add a new definition of "sensitive personal data" and to make new provisions prohibiting the collection, holding, processing and use of sensitive personal data except under prescribed circumstances.

Reasons for the Proposal

1. The Ordinance as it currently stands does not contain provisions differentiating personal data that are "sensitive" from those that are not. The Law Reform Commission ("LRC") had considered the issue in 1994[1] on the feasibility of imposing specific restrictions on the collection of specific categories of data. Three mechanisms[5] to restrict the collection of special categories of data were raised, namely by (i) outright ban on collection; (ii) prior approval of the data protection authority to be obtained; or (iii) prior approval from data subject. Option (i) was not viewed as a realistic option while option (ii) was considered as encouraging bureaucracy by involving the protection authority in a consent role. The requirement of prior consent of data subject for collection of sensitive personal data, including collection from third parties as proposed in option (iii) was taken to be the most viable option.

2. However, the public response at that time showed concerns over the practicability of requiring the data subject's express consent as a prerequisite to the collection of sensitive personal data and the difficulties in identifying and classifying data that were sensitive. That was the situation before the EU Directive came into play.

3. Article 8(1) of the EU Directive 95/46/EC[6] provides that member states shall prohibit the processing of personal data *"revealing racial or ethnic*

---

1 *Report on Reform of the Law Relating to the Protection of Personal Data*, 1994 http://www.hkreform.gov.hk/en/docs/rdata-e.pdf

5 *See paragraph 9.50 of the LRC's Report on Reform of the Law Relating to the Protection of Personal Data*, 1994 http://www.hkreform.gov.hk/en/docs/rdata-e.pdf

6 The *"Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data"* issued on 24 October 1995 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life". These kinds of personal data are accorded higher degree of sensitivity under the EU Directive for which special rules for processing apply.

4. According to international practice and standards, certain kinds of personal data are regarded as inherently sensitive, e.g. one's sexual inclination or medical or health data, particularly in view of the degree of harm that may be inflicted upon the data subject on their wrongful use and handling[7]. The overseas privacy legislations that contain provisions that deal with the handling of sensitive personal data generally prescribe for strict preconditions to be met and these include where the data subject consents[8], where the collection is required by law[9], or where the collection is necessary to prevent or lessen a threat to the life or health of an individual[10].

5. Now that the EU Directive has been operative for more than ten years and that a number of countries have in their respective privacy laws, imposed specific restrictions on the processing of sensitive personal data, the doubts and concerns about the feasibility of imposing restrictions should have been resolved.

6. The Commissioner considers the following factors relevant in classifying

---

7 For instance, section 2 of the UK Data Protection Act and section 6 of the Australian Privacy Act. http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_2#pt1-l1g2, http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/framelodgmentattachments/1B0AD21B8A87AD58CA2576080018DAEF

8 Paragraph 1 of Schedule 3 of the UK Data Protection Act 1998 refers http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_10#sch3. See also Principle 10.1(a) of the National Privacy Principle http://www.privacy.gov.au/publications/npps01.html#npp10 on sensitive information found in Schedule 3 of the Privacy Act 1988 of Australia.

9 See, for example, paragraph 2(1) of Schedule 3 of the UK Data Protection Act 1998 which allows processing of sensitive personal data where it is necessary for exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_10#sch3. Principle 10.1(b) of the National Privacy Principle of Australia has similar provision to allow for collection of sensitive information where the collection is required by law. http://www.privacy.gov.au/publications/npps01.html#npp10

10 For instance, section 54 of the Privacy Act 1993 of New Zealand empowers the Commissioner to authorize an agency the collection, use, or disclosure of personal information if the Commissioner is satisfied that in the special circumstances of the case, the public interest outweighs to a substantial degree the interference with the privacy of the individual or the collection, use or disclosure involves a clear benefit to the individual concerned that outweighs any interference with the privacy of the individual http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM297419.html. See also paragraph 3 of Schedule 3 of the UK Data Protection Act 1998 allowing processing where it is necessary to protect the vital interests of the data subject or another person in case where consent cannot be given or unreasonably withheld by the data subject. http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_10#sch3

certain personal data as “sensitive” and attaching a higher standard of care in their handling :

(i) It is consistent with the legislative intent to provide a higher degree of protection towards more sensitive personal data. In particular, under DPP4 a higher degree of care is called for in handling sensitive personal data given the gravity of harm that may be inflicted upon the data subject as a result of leakage or disclosure of such data to third parties;

(ii) Limiting the processing of sensitive personal data to specified circumstances would narrow down the broadness of scope that may be relied upon when personal data are collected and used for directly related purposes;

(iii) By classifying certain categories of data as “sensitive data” for which special rules in handling and processing apply, it gives better safeguard to those kinds of data against indiscriminate use and inappropriate handling;

(iv) The statutory recognition of “sensitive data” under the Ordinance is in alignment with international privacy standards and practice; and

(v) Amending the Ordinance to provide special treatment for sensitive personal data is in compliance with Article 8 of the EU Directive, thereby enabling the Ordinance to pass the EU adequacy test.

7. The Commissioner proposes to include biometric data as sensitive personal data. Biometric data, such as iris characteristics, hand contour reading and fingerprints are by virtue of their unique and unchangeable nature, renders the identity of an individual practicably ascertainable, meeting the definition of “personal data”. With the increasing use of fingerprint scanners for a vast array of commercial and human resources management purposes, it warrants special care and attention for the protection against such issues as identity theft.

8. The Commissioner also proposes that “political affiliation” instead of “political opinion” be classified as sensitive personal data for the following reasons :

(i) The term “political opinion” tends to be conceptual and vague and is potentially contentious since different persons may form

different views as to what constitutes political as opposed to non-political opinion;

(ii) "Political opinion" being a form of manifestation of the fundamental right of freedom of speech is not to be singled out from other forms of expression of personal opinions for which general rules on compliance with the Ordinance shall apply;

(iii) In contrast, the term "political affiliation", i.e. association with certain political parties in Hong Kong, is one which can be more easily established and shown; and

(iv) There are public concerns that a name list of persons who are affiliated with their political parties is sensitive information which should be protected. Distinction should be made from the list of members filed with public registries, such as the Companies Registry pursuant to the Companies Ordinance. According to our proposed amendments, such information which is available from public search is taken to fall within the exception of being *"data being manifestly made public by the data subject"* and hence not "sensitive" anymore.

9. As to whether "sensitive data" shall include the commission or alleged commission of an offence and any proceedings relating to an offence alleged to have been committed, etc, it is noted that the EU Directive is silent on its inclusion. Although the UK Data Protection Act has treated the same as "sensitive personal data", the inclusion or not depends very much on policy considerations such as:-

(i) The general public's perception of the privacy intrusiveness of such data;
(ii) The incidences of misuses;
(iii) The likely damage to be caused;
(iv) The protection of the public interest to be informed;
(v) The fact that such information may be obtainable from public domain, e.g. from court judgments and action list searchable by public, etc.

As the LRC in its Report on Civil Liability for Invasion of Privacy has suggested, it should be a subject of amendment under the Rehabilitation of Offenders Ordinance, Cap 297. That said, the Commissioner is open-minded as to whether they should be classified as "sensitive personal data".

10. By virtue of the sensitive nature of these personal data, the obtaining of the prescribed consent of the data subject with clearly defined excepting circumstances gives better personal data privacy safeguard against indiscriminate and improper handling. The data subject's right of information self-determination, particularly over his sensitive personal data, should be respected and upheld.

Suggested Amendments

(A) To add a new definition of "sensitive personal data" under section 2(1) of the Ordinance as follows:-

"sensitive personal data" means personal data consisting of information as to –

(i) the racial or ethnic origin of the data subject;
(ii) his political affiliation;
(iii) his religious beliefs and affiliations;
(iv) membership of any trade union (within the meaning of the Trade Unions Ordinance, Cap 332);
(v) his physical or mental health or condition;
(vi) his biometric data; or
(vii) his sexual life.

(B) That a new section 4A be added immediately after section 4:-

"4A. Handling of sensitive personal data

(1) Without prejudice to and without limiting the operation of the other provisions of this Ordinance and the obligations of data users under this Ordinance, the collection, holding, processing and use of sensitive personal data are prohibited unless—

(a) with the prescribed consent of the data subject;
(b) the collection, holding, processing or use of the data is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data user;
(c) necessary for protection of the vital interests of

the data subject or of another person(s) in situation where—

(i) prescribed consent cannot be given by or on behalf of the data subject;

(ii) the data user cannot reasonably be expected to obtain the prescribed consent of the data subject; or

(iii) in order to protect the vital interests of another person(s) in situation where prescribed consent of the data subject has been unreasonably withheld;

(d) in the course of the data user's lawful function and activities with appropriate safeguard against transferring or disclosing to third parties without prescribed consent of the data subject;

(e) the data has been manifestly made public by the data subject;

(f) the collection, holding, processing or use of the data is necessary for medical purposes and is undertaken by a health professional or a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional;

(g) insofar as the data relating to racial or ethnic origin is concerned, the collection, holding, processing or use of the data is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained; or

(h) the collection, holding, processing or use of the data is necessary for the purpose of, or in connection with any legal proceedings including the purpose of obtaining legal advice or otherwise necessary for the purpose of

establishing, exercising or defending legal rights.

(2) In this section, the term "medical purposes" includes the purposes of preventive medicine, medical diagnosis, medical research, the provision of care and treatment and the management of health care services."

(C) In the absence of specific offence provision, contravention of the new section 4A will be caught as an offence under section 64(10) of the Ordinance.

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reason:-

Given the different perceptions as to what should be treated as "sensitive" personal data, the Commissioner is open-minded on the kinds of personal data that are to be included as "sensitive" personal data, the scope of the excepting circumstances, for instance, whether public interest should be a valid ground of exemption and the level of penalty. He also welcomes any feedbacks on the social, economic or political impacts that the proposed changes will bring and the legitimate expectation of the general public on personal data privacy in respect of specific kinds of personal data.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 2

To add a new definition of "data processor" and to provide for the respective obligations and duties of a data processor and data user to comply with the requirements of the Ordinance.

Reasons for the Proposal

1. Currently, there is no such term as "data processor" under the Ordinance. Under section 2(12) of the Ordinance, a person is not taken to be a data user if he holds, processes or uses personal data solely on behalf of another person but does not have any of his own purposes to hold, process or use the data. Not being a data user, it naturally follows that the Ordinance therefore does not have application to such person[1].

2. Under Article 16 of the EU Directive 95/46/EC, a duty of confidentiality is imposed upon the "data processor" and the "data controller" shall implement appropriate technical and organizational safeguards to protect the personal data against accidental or unauthorized alteration, disclosure or access, in particular where the processing involves the transmission of data over a network and the level of security shall be appropriate to counter the risks posed by such processing having regard to the nature of the data involved.

3. UK followed the EU Directive and its Data Protection Act specifically provides for the definition of "data processor" which essentially means any person who processes the data on behalf of the data controller. Insofar as personal data are entrusted to the processor for processing, it shall assume the role of data controller. The UK data protection principles impose duty on data controller to implement appropriate technical and organizational measures include (i) the choosing of a data processor providing sufficient guarantees in respect of technical and organizational measures governing the processing of the data; and (ii) the taking of reasonable steps to ensure compliance with those measures by the data

[1] As it becomes clear that section 4 of the Ordinance has no application which obliges a data user to act or engage in practice in compliance with the requirements of the Ordinance http://www.pcpd.org.hk/english/ordinance/section_08.html#sect4.

processor. Similarly in Canada, explicit obligations are imposed upon the organization to make use of contractual or other means to ensure compliance of the Personal Information Protection and Electronic Documents Act by such third parties as subcontractors and agents[2].

4. The Australian privacy legislation has also imposed duty upon a record keeper that if it is necessary for the records containing personal information to be given to a person in connection with the provision of service to the record keeper, it should do "everything that is reasonable within its power to prevent unauthorized use or disclosure of information contained in the records"[3].

5. The Commissioner considers it necessary to regulate the act and practice performed by a data processor for the following reasons :

   (i) The increasing trend of sub-contracting and entrusting the data processing works to a third party has exposed the personal data to a higher risk of unauthorized or accidental access, handling and processing;

   (ii) Complaint cases handled by the Commissioner show that there are very often no or insufficient security safeguards being imposed upon a data processor when personal data are transferred to it for handling;

   (iii) The damage to be suffered by the data subjects can be significant and far-reaching particularly when it involves electronic processing of the data. The investigation report published by the Commissioner on IPCC data leakage incident is a case in point[4];

   (iv) The role of the data processor is akin to that of an agent and section 65(2) of the Ordinance has provided that the principal shall be liable for the act done or practice engaged in by his agent. The Ordinance, however, does not prescribe for any specific privacy protective measures to be adopted by the agent; and

   (v) The provision of specific duty and obligation upon a data processor

---

2 Personal data privacy afforded under the Personal Information Protection and Electronic Documents Act had passed the EU's adequacy test by a decision passed on 20 December 2001 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:002:0013:0016:EN:PDF.

3 Information Privacy Principle 4 of the Federal Privacy Act http://www.privacy.gov.au/publications/ipps.html#d

4 The report can be downloaded from the webpage: http://www.pcpd.org.hk/english/publications/files/IPCC_e.pdf

and data user is in alignment with international standard and practice.

6. The Commissioner finds it necessary to impose a duty on the part of the data processor to observe and comply with DPPs 2(2), 3 and 4, i.e. to ensure the erasure of personal data no longer required for fulfillment of the purpose of use, the proper use of the personal data for original or directly related purpose and the taking of all practicable steps to ensure the security and safekeeping of the data. These are the primary privacy issues that the data processor should take heed of.

7. As for the duty that is to be imposed upon the data user, the Commissioner proposes that DPP4 be amended to specify the security measures incumbent upon the data user to take when contracting out or outsourcing the processing of data to third parties.

Suggested Amendments

That section 2(1) of the Ordinance be amended to add a new definition of "data processor" which means a person who holds, processes or uses personal data solely on behalf of a data user and does not hold, process or use those data for any of his own purpose.

That section 4 be amended to specify the obligation of a data processor not to do an act or engage in a practice that contravenes DPPs 2(2), 3 and 4.

That DPP4 in Schedule 1 of the Ordinance be amended so that where personal data are transferred to a data processor for holding, processing or use, the data user shall use contractual or other means to provide a comparable level of security protection while the personal data are being held, processed or used by the data processor engaged by the data user.

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reason:-

The proposed amendments introduce new obligation on data processors and impose additional duties upon data users under DPP4. In view of the social and economic impact that it will have on data users and persons who carry on the business of data processing, the issue warrants public consultation.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 3

To define the word "crime" and "offence" under the Ordinance to mean Hong Kong crime and offence and also include those for which the Mutual Legal Assistance in Criminal Matters Ordinance, Cap 525 apply.

Reasons for the Proposal

1. The Ordinance as it currently stands does not define the words "crime" and "offence" which are found in the exemption provision of section 58 of the Ordinance. Doubts were cast on the ambit of the exemption under section 58 as to whether it was wide enough to cover overseas crime and offence so that a data user can properly invoke the exemption, for instance, in disclosing personal data to an overseas law enforcement agency for investigation of a foreign crime.

2. The matter was canvassed and studied by the Commissioner in handling the complaint lodged against Yahoo! Holdings (Hong Kong) Limited on alleged disclosure of personal data in the PRC to the PRC State Security Bureau for investigation of a crime of leakage of state secret. One question for the Commissioner to consider was whether the exemption provisions under section 58 of the Ordinance could be applicable to Yahoo in disclosing the personal data. A full report of the complaint case can be downloaded from the PCPD's website[1].

3. Section 58(1)(a) and (b) of the Ordinance provide for the exempted purposes of "the prevention or detection of crime" and "the apprehension, prosecution or detention of offenders". In Hong Kong, the Mutual Legal Assistance in Criminal Matters Ordinance, Cap 525 ("MLA Ordinance") regulates the provision and obtaining of assistance in criminal matters between Hong Kong and places outside Hong Kong. Section 5(1)(g) of the MLA Ordinance provides that "a request by a place outside Hong Kong for assistance under this Ordinance shall be refused if, in the opinion of the Secretary for Justice, the request relates to an act or omission that, if it had occurred in Hong Kong, would not have constituted a Hong Kong offence".

[1] See report at the link : http://www.pcpd.org.hk/english/publications/files/Yahoo_e.pdf

4. The Commissioner had drawn reference to provisions found in overseas privacy legislations. In Australia, disclosure of personal information by a private sector organization is allowed under the National Privacy Principle 2.1(g) of the Australian Privacy Act 1988 when it is "required or authorized by or under any law". The Mutual Assistance in Criminal Matters Act 1987 enables the Commonwealth of Australia to provide international assistance in criminal matters upon request of a foreign country and disclosure pursuant thereto is viewed as "authorized by law" covered by the Act[2].

5. In New Zealand, an exception to disclosure of personal data is provided under Information Privacy Principle 11(e) which allows disclosure "to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution and punishment of offences". The term "public sector agency" is further defined in a way that it could only be New Zealand public body.

6. The Commissioner finds important public policy consideration when construing "crime" or "offenders" in section 58. Having regard also to the territorial principle of the Ordinance, the Commissioner finds it sensible, prudent and reasonable to interpret the words "crime" or "offenders" under section 58(1)(a) and (b) to mean crime or offence under Hong Kong laws and it also extends to cover cases to which the MLA Ordinance is applicable.

7. The Commissioner's interpretation of the meaning of the words "crime" and "offenders" was heard by the Administrative Appeals Board ("AAB") in Administrative Appeals No. 16/2007. At paragraph 97 of the Decision, it states:-

> *"… it is common ground between the Commissioner and the Appellant that the exemption in section 58 of the Ordinance cannot be invoked in the present case. We accept that the crime committed by the Appellant in the PRC did not amount to a crime under the laws of Hong Kong. Accordingly, it is not necessary to dwell upon the applicability of section 58 in the instant case."*

8. In the absence of a clear definition of the word "crime" and the lack of

---

[2] See Principle 2 in Schedule 3 of the Privacy Act 1988, Australia http://www.comlaw.gov.au/ComLaw/legislation/actcompilation1.nsf/0/43675D27C7449FB1CA2575C50002F647/$file/Privacy1988_WD02.pdf. Principal 2.1(g) thereof allows use and disclosure of personal information where it *"is required or authorized by or under law"*.

AAB or judicial ruling, it would be difficult for the data user to assess whether an exemption provision under section 58(1) and (2) can be properly invoked, especially when it is requested by an overseas law enforcement agency to disclose certain personal data for the investigation of a foreign crime. A data user is disclosing personal data at the peril of contravention of the requirement of the Ordinance should an exemption provision be wrongly relied upon and invoked. The Commissioner finds it necessary and therefore proposes that the Ordinance be amended to include specific definition on the words "crime" and "offenders".

Suggested Amendment

That section 2(1) of the Ordinance be amended to add a new definition of "crime" to mean (i) an act or omission that is punishable as an offence under the laws of Hong Kong or (ii) an act or omission for which legal assistance under the Mutual Legal Assistance in Criminal Matters Ordinance, Cap 525 has been sought and obtained. And the meaning of "offender" and "unlawful" shall be construed accordingly.

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reason:-

Issues of public interest that public's views and opinions should be solicited.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 4

To expand the definition of "relevant person" by including a guardian appointed under sections 44A, 59O and 59Q of the Mental Health Ordinance.

Reasons for the Proposal

1. The Ordinance permits the lodging of complaint to the Commissioner by a relevant person on behalf of the affected data subject[1] and also permits the making of a data access[2] and data correction request[3] by the relevant person on behalf of the individual concerned. The definition of "relevant person" under section 2(1) of the Ordinance means the person who has parental responsibility for the minor or the person who is appointed by a court to manage the affairs of the individual.

2. In the case where lawful guardian is appointed under the Mental Health Ordinance ("MHO"), the definition of "relevant person" under the Ordinance is found to be insufficient to cover such guardian so appointed under sections 44A, 59O and 59Q of the MHO for the following reasons:-

   (i) under section 44A of the MHO, a guardian may be appointed by a court or magistrate and it is arguable whether an appointment by a magistrate can for the purpose of the definition of "relevant person" be regarded as being made by a court;

   (ii) guardianship orders made under sections 59O and 59Q of the MHO are made by the Guardianship Board, which is a body corporate established under the MHO and is not a court; and

   (iii) a guardian appointed under sections 44A, 59O or 59Q of the MHO may exercise one or more powers specified in sections 44B or 59R respectively. Thus, the guardian's powers are specific and may not be wide enough to cover the managing of the data subject's affairs[4].

---

1 Section 37 of the Ordinance http://www.pcpd.org.hk/english/ordinance/section_46.html
2 Section 18 of the Ordinance http://www.pcpd.org.hk/english/ordinance/section_24.html
3 Section 22 of the Ordinance http://www.pcpd.org.hk/english/ordinance/section_29.html
4 In *AAB No. 27/2005*, a guardian appointed by the Guardianship Board under section 59O of the

3. In order to accord sufficient protection to this class of data subjects so that their rights to complain and to make data access and correction requests under the Ordinance are not deprived, it is recommended that the term "relevant person" be amended to cover guardian appointed under the MHO. The Commissioner also envisages that there are situations that it will be in the interests of the data subjects for the guardian appointed under the MHO to have access to and correct the relevant personal data of the data subject. Proposal was made by the Guardianship Board for amending the Ordinance accordingly.

Suggested Amendment

That the definition of "relevant person" under section 2(1) of the Ordinance be amended to include guardians appointed under the MHO.

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Not recommended for the following reason:-

The amendment is straight forward to close loopholes and is unlikely to be controversial.

Mental Health Ordinance, Cap 136 http://www.legislation.gov.hk/blis_pdf.nsf/6799165D2FEE3FA94825755E0033E532/4D4C0652AC60B789482575EE00433474/$FILE/CAP_136_e_b5.pdf was held not to be a "relevant person" under the Ordinance because : (i) the Guardianship Board is not a court and (ii) the appointment did not empower the guardian to manage the affairs of the incapacitated person. Hence, the guardian could not lodge a complaint under section 37 on behalf of the incapacitated person.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 5

To allow the "relevant person" of a minor or a mentally incapacitated person to give prescribed consent on behalf of the data subject when use of the personal data involves a clear benefit to the data subject.

Reasons for the Proposal

1. The Ordinance as it presently stands does not allow for the giving of consent by a relevant person on behalf of a minor or one who is incapable of managing his own affairs. The "prescribed consent" under DPP3 must therefore be one that comes from the data subject.

2. The Commissioner takes the view that "prescribed consent" given under DPP3 must premise on the prerequisite that the data subject should be capable of giving a voluntary and informed consent. Where the disparity in bargaining powers is obvious and when it is doubtful that undue influence will exist, these are relevant factors that the Commissioner will consider as to whether voluntary and express consent has indeed been given.

3. Given the vulnerability of the class of data subjects, i.e. a minor or one who is mentally incapacitated, it is doubtful whether they can genuinely appreciate the privacy impact on the change of use of their personal data in every circumstance. Particularly, it is important to consider whether the data subject in question has the necessary mental capacity to understand what is being offered to him. There may be practical difficulties in deciding whether the data subject has the requisite mental capacity and they are illustrated in the following examples:-

   Example 1

   The parent of a minor complained that the medical doctor had disclosed his son's medical test result to the principal of the school where his son was studying which information was later being used by the school for expelling the child. It was however revealed that the minor had in fact signed a form agreeing to the release of the test result to the school. The

disclosure with prescribed consent of the minor was therefore not a contravention of DPP3.

Example 2

A minor divulged personal information in confidence to a social worker in the course of seeking his advice and on the explicit understanding that it would not be disclosed to the minor's parents. The parents requested for disclosure of such information held by the social worker who in disclosing the same ran the risk of breach of DPP3 as well as the professional duty of confidence although it may be in the best interest of the minor for the social worker to do so.

4. The above shows that instead of drawing an artificial age distinction to differentiate those data subjects who have the requisite mental capacity to give consent from those who cannot, the Commissioner finds it more appropriate that each individual should be separately assessed in deciding whether he is competent to give prescribed consent.

5. The "Gillick competency" test introduced in the UK landmark decision of *Gillick v West Norkfolk and Wisbech Area Health Authority and Another [1986] 1AC112* sheds light on the proper test to apply. The case concerns the prescription of contraception by medical doctor to a minor at her request. The test essentially requires that a child could only give consent if he or she had a "sufficient understanding and intelligence" to enable him or her to fully understand the medical treatment that is proposed.

6. The right of individual, regardless of age, to give consent to handle his own personal data or information are generally recognized by overseas privacy legislations. Excepting circumstances are, however also allowed for in protecting the best interests of the minor by either empowering the relevant authority to exempt certain acts from being treated as contravention or by giving statutory exemption to the use and disclosure of personal data under prescribed circumstances.

7. There are situations that the giving of consent by one with parental responsibility or by his legal guardian serves the best interest of the data subject, e.g. in deciding the proper course of medical treatment to be received in safeguarding the vital interest of the data subject or for managing his affairs in a way that best protects the data subject's financial or other interests. Public interest exists to protect the privacy of these vulnerable classes of data subjects in accepting consent given by the

relevant persons on behalf of the data subjects when it is done in the best interest of the data subjects in question.

8. In deciding what is in the "best interest" to serve, the duty lies upon the person who gives such consent on behalf of the minor to show that it serves a clear benefit to the data subject having regard to the extent of intrusion into personal data privacy of the data subject and the benefits or privileges to be derived. Reasonableness and proportionality are the benchmarks to measure. The Commissioner would adopt an objective test in making his decision if a complaint is brought before him.

9. Prescribed consent to be given by a relevant person on behalf of the data subject should be allowed under the following two conditions:

   (i) That the data subject is one who is incapable of giving prescribed consent as being one who does not achieve a sufficient understanding or intelligence to enable him to fully understand what is being proposed to him; and

   (ii) That the proposed change of use of the personal data involves a clear benefit to the data subject.

10. A data user who uses personal data of the data subject in reliance of consent given by the relevant person must act with caution. Any wrongful reliance by the data user will be liable for contravention of the requirement of the Ordinance. Therefore, a data user should make necessary enquiries in order to satisfy that the two conditions are fulfilled. So long as the data user has reasonable grounds to believe that the two conditions are fulfilled, this might avail the data user a ground of defence for any claim filed by the data subject.

Suggested Amendments

That the meaning of "prescribed consent" under section 2(3)(b) of the Ordinance be amended to include consent given by a relevant person in the following circumstances:-

"Section 2(3)(b)—

(i) A person is incapable of giving a prescribed consent for the purpose of this Ordinance if he does not have a sufficient understanding and

intelligence to enable him to understand fully what is proposed to him.

(ii) Where sub-paragraph (i) applies and provided that the use of the personal data involves a clear benefit to the data subject, the person referred to in paragraphs (a) or (b)[1] (where appropriate) of the definition of "relevant person" in section 2(1) may give prescribed consent on behalf of the data subject.

(iii) The data user to whom prescribed consent is given pursuant to sub-paragraph (ii) shall, unless there is evidence to the contrary, treat the consent as good as the one given by the data subject with capacity.

(iv) In proceedings brought under this Ordinance against any person for a contravention of section 30(1) or data protection principle 3, it shall be a defence for that person to prove that he had reasonable grounds to believe that the conditions under sub-paragraphs (i) and (ii) are fulfilled.

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reason:-

The issue has significant privacy impact as it brings important changes to the concept of "prescribed consent" in allowing a relevant person to give it on behalf of the data subject. There may be policy consideration as to the likelihood of abuse by the relevant person and the sufficiency of protection to the data users and data subjects alike.

[1] Paragraph (a) is "where the individual is a minor, a person who has parental responsibility for the minor". Paragraph (b) is "where the individual is incapable of managing his own affairs, a person who has been appointed by a court to manage those affairs".

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 6

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.

Reasons for the Proposal

1. The Yahoo's case gives rise to concern on the scope of application of the Ordinance.

2. The Ordinance as it presently stands is unclear as to whether it applies to cases where the act of collection, holding, processing and use of personal data takes places wholly outside Hong Kong. Section 39(1)(d) provides that where none of the conditions specified is fulfilled in respect of the act or practice complained of, the Commissioner may refuse to carry out or continue with an investigation initiated by a complaint. One of the conditions specified under section 39(1)(d)(i)(B) is where "the relevant data user was able to control, in or from Hong Kong, the collection, holding, processing or use of the personal data concerned". It should however be noted that section 39(1)(d) is not a provision dealing with extra-territorial application of the Ordinance and *"it does not provide the answer as to whether the Ordinance may have extra-territorial application"*[1].

3. Where personal data are wholly collected, held, processed and used by an organization or a person outside Hong Kong, the act or practice is likely to be subject to the applicable laws at the place that the act takes place or the practice is engaged in.

4. By the operation of the territorial principle, certain territorial link with Hong Kong should exist in order for the Ordinance to apply. The mere presence in Hong Kong, without more, of a person who is able to control his business operations overseas should not thereby render the person a data user subject to the jurisdiction of the Ordinance. However,

[1] In AAB No.16/2007, although the Board did not rule on the issue of extra-territorial application of the Ordinance, the above comments were made by the Board.

according to the decision in AAB No. 16/2007, the Administrative Appeals Board decided that insofar as the person satisfies the definition of "data user" under the Ordinance exercising control over the personal data "*in or from Hong Kong*", the Ordinance shall apply notwithstanding that none of the acts of collection, holding, processing or use of the personal data takes place in Hong Kong[2].

5. Following the rationale of the AAB decision, a data user will face the dilemma of either breaching the Ordinance if it authorizes disclosure of the personal data to a foreign law enforcement authority or faces the legal consequence (sometimes involving criminal sanction) under the applicable foreign law if it fails to comply with the lawful order issued under that law.

6. Apart from the above anomaly, practical difficulty will also be encountered by the Commissioner in respect of evidence gathering of such extra-territorial act or practice and the effective compliance with the enforcement notice, if any, issued under section 50 of the Ordinance against the relevant data user.

7. Section 33 of the Ordinance, which prohibits the transfer of personal data outside Hong Kong, provides in subsection (1) that it applies to personal data the collection, holding, processing or use of which takes place in Hong Kong or is controlled by a data user whose principal place of business is in Hong Kong. Although this section is not yet in operation, its spirit is premised on the fact that personal data are held in Hong Kong before being transferred overseas.

8. A study of overseas privacy legislations shows that most of these jurisdictions have also adhered to the territorial principle.

9. Notwithstanding the decision given in the said AAB appeal, the Commissioner finds it advisable to exclude from the application of the Ordinance where none of the acts of collection, holding, processing and use of personal data takes place in Hong Kong.

Suggested Amendment

A new section be added to the Ordinance to provide that the Ordinance shall

---

[2] In AAB No. 16/2007, the Board decided that Yahoo! Hong Kong Limited was a "data user" under the Ordinance and was responsible for acts committed by its agent operating in the PRC. See paragraph 89 of the decision.

not apply to an act or a practice that relates to personal data the collection, holding, processing and use of which occur wholly outside Hong Kong. This provision is without prejudice to and does not limit the application of section 33.

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reason:-

The issue touches on the question of jurisdiction and in view of the vast number of business practices which involve the keeping of a liaison office in Hong Kong while the collection, holding, processing and use of personal data pertinent to its businesses happened wholly outside Hong Kong, the matter deserves public scrutiny and deliberations.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 7

That personal data held or otherwise placed in the custody of a court or judicial officer in the course of the exercise of judicial functions shall be exempted from the application of the Ordinance.

Reasons for the Proposal

1. Personal data will be handled by the courts and the judicial officers in the course of the exercise of judicial functions. Since the Ordinance does not contain express provision exempting such act or practice from the application of the Ordinance, complaints have been received by the Commissioner in relation to the collection and/or disclosure of personal data by judges during court hearings as well as the making of data access request for the supply of judges' notes and records held by courts or registries in relation to particular proceedings.

2. Although the Ordinance does not contain provision exempting personal data held by judicial officers in exercise of their judicial function from application of the Ordinance, the Commissioner finds the exercise of his enforcement powers in those situations to be in conflict with Article 85 of the Basic Law.

3. Article 85 of the Hong Kong Basic Law provides that "the courts of the HKSAR shall exercise judicial independence, free from any interference. Members of the judiciary shall be immune from legal action in the performance of their judicial functions".

4. Section 2A of the Interpretation and General Clauses Ordinance, Cap 1, Laws of Hong Kong, clarifies the position by providing that all laws previously in force shall be construed with such "modification, adaptation, limitations and exceptions" as may be necessary so as not to contravene the Basic Law.

5. In an appeal lodged with the AAB[1] concerning the alleged improper disclosure of the claimant's medical certificate by a tribunal to the

[1] AAB No. 39/2004

defendant, the medical certificate in question was produced by the claimant to the tribunal in support of his request for adjournment of the hearing due to sickness. The AAB held that it was not the role of the Commissioner to oversee the Judiciary and the Ordinance has no application to judicial acts.

6. Reference was also made to the overseas privacy legislations. In UK, for instance, section 32 of the Freedom of Information Act provides that "any document created by a court or a member of the administrative staff of a court for the purposes of proceedings in a particular case or matter" is exempt information. It gives the public authorities a valid ground to refuse access to exempt documents. Similar provision is found in section 10 of the Information Privacy Act, Australia which exempts from its application the holding, management and use, etc. of personal information by a court or tribunal or registry and its staff in relation to the exercise of the judicial or quasi judicial functions.

7. Having regard to the Basic Law, the AAB decision and the overseas legislations, it is found appropriate to specifically exclude from the application of the Ordinance any act or practice concerning personal data handling by the courts, tribunals and judicial officers in the exercise of judicial functions.

Suggested Amendments

It is proposed to create a new provision to exclude from the application of the Ordinance the following:-

(a) personal data held by or otherwise placed in the custody of a court for the purpose of proceedings in a particular cause or matter;
(b) personal data contained in any document created by a court or a member of the administrative staff of a court, for the purposes of proceedings in a particular cause or matter.

"Court" means any court, magistrates' court, tribunal or body exercising judicial function.

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Not recommended for the following reason :

Judicial independence and immunity are entrenched in the Basic Law. There is unlikely to be controversy.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 8

That the Commissioner be expressly conferred with the power to investigate and prosecute offences under the Ordinance.

Reasons for the Proposal

1. Under the current provisions of the Ordinance, the Commissioner has no power to investigate criminal offence and he can only refer the case to the police for investigation with follow up prosecution action, if any, undertaken by the Secretary for Justice.

2. Typical cases so far referred by the Commissioner to the police involve violation of the following provisions of the Ordinance:

   (j) the breach of section 19(1) by a data user who fails to comply with a data access request not later than 40 days after receiving the request;

   (ii) the breach of section 34 by a data user in carrying out direct marketing activities after the data subject has "opted out" from such activities;

   (iii) the breach of section 64(7) by a data user who contravenes an enforcement notice served upon it; and

   (iv) the breach of section 64(9) by a data user who makes false or misleading statement to the Commissioner.

3. There are other provisions of the Ordinance, the breach of which constitutes an offence. For example, the breach of section 23 in relation to data correction request attracts criminal sanction under section 64(10). The same sanction also applies to failure on the part of a data user to erase personal data no longer required under section 26 or to file a data user return under section 14. In addition, a data user carrying out a matching procedure in breach of a condition specified by the Commissioner is an offence under section 64(5).

4. The following are factors justifying the giving of an express power to the Commissioner to investigate and prosecute an offence under the Ordinance:-

(i) Since the time to lay prosecution as prescribed under section 26 of the Magistrates Ordinance is 6 months from commission of the offence, sometimes it would be impracticable for the police and the Department of Justice to meet the strict statutory time limit after the Commissioner's referral of the complaint;

(ii) The Commissioner who possesses the first hand information obtained in the course of his complaint investigation could act swiftly to deal with suspected commission of the offence; and

(iii) Charged with the regulatory role, the Commissioner is capable of interpreting and applying the provisions of the Ordinance and could appraise of any given situation by assessing the weight and relevancy of the evidence with ease and confidence.

5. In order that the new power can be exercised efficiently and effectively and in view of the additional call on resources, the Commissioner also proposes that the Court should be given power to award costs against a party convicted of an offence to pay the Commissioner the whole or part of the costs and expenses of the investigation. This has been the approach adopted by the recently passed Unsolicited Electronic Messages Ordinance[1] which is an useful example to follow.

Suggested Amendments

(i) To create express powers for the Commissioner to investigate and prosecute offences under the Ordinance.

(ii) To add a new section so that the Court may order a party convicted by the Court of an offence to pay the Commissioner the whole or part of the costs and expenses of investigation.

[1] See section 43 of the Unsolicited Electronic Messages Ordinance. http://www.legislation.gov.hk/blis_pdf.nsf/6799165D2FEE3FA94825755E0033E532/BE5AA57E2A0358C7482575EF00201941/$FILE/CAP_593_e_b5.pdf

The Commissioner’s Disposition

Supported.

Public Consultation : Recommended or Not

Recommended because of the following reason:-

The proposed amendments extend the powers of the Commissioner and public scrutiny is required.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 9

That the Commissioner be conferred with a specific power to impose reasonable charges for services rendered and for providing publications.

Reasons for the Proposal

1. While the present practice of accepting gifts or donations on ad hoc basis is expressly permitted under section 8(2)(d) of the Ordinance, there is no provision under the Ordinance that empowers the Commissioner to charge for fees in respect of services rendered by him in discharge of his functions and powers.

2. The fee earning capacity of the Commissioner, if properly exercised, can achieve and enhance the more efficient discharge of the Commissioner's powers in the following aspects:

   (i) That more promotional and educational projects or programmes on a larger scale and regular basis can be launched or participated by the PCPD in promoting awareness of personal data privacy and compliance with the Ordinance;

   (ii) That medium to long term commitments can be entered into with relevant professional bodies or industry sectors to engage or undertake training courses, seminars or workshops;

   (iii) Frequent and regular revenue generated as a result will provide resources to enable the Commissioner to undertake other non-profit making promotional activities for public educational purposes; and

   (iv) More diversified range of services and activities catering for the needs and demands of the public as well as interested groups can be undertaken.

3. Other regulatory bodies, such as the Ombudsman and the Equal Opportunities Commission have similar fee charging power under their respective ordinances. For example, section 9A of the Ombudsman

Ordinance (Cap 397) empowers the Ombudsman to charge any person reasonable fee in respect of services approved by the Director of Administration. Section 65 of the Sex Discrimination Ordinance (Cap 480) enables Equal Opportunities Commission to impose reasonable charges for educational or other facilities or services made available by it.

Suggested Amendments

That section 8(2) of the Ordinance be amended to provide for an express power for the Commissioner to impose reasonable charges for:-

(i) undertaking educational, promotional or other activities or services;

(ii) providing pamphlets, booklets or other publications; and

(iii) such other services or activities which appear to the Commissioner necessary or expedient for the performance of his functions.

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Not recommended for the following reason :

Unlikely to raise controversy since the proposed power is similar to those already enjoyed by the Equal Opportunities Commission and the Ombudsman.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 10

That the guidelines prepared and published by the Commissioner under section 8(5) of the Ordinance shall also provide guidance to data subjects.

Reasons for the Proposal

1. Section 8(5) empowers the Commissioner to prepare and publish by notice in the Gazette, "for guidance of data users", guidelines indicating the manner in which the Commissioner proposes to perform any of his functions or exercise of any of his powers under the Ordinance.

2. In exercise of the power conferred under section 8(5), the Commissioner had issued *Privacy Guidelines : Monitoring and Personal Data Privacy at Work* in December 2004 which gives practical guidance to data users and data subjects when employer intends to collect personal data of employees through monitoring activities carried out by it.

3. Section 8(5) as it presently stands is unnecessarily narrow as it has omitted to mention that the guidelines issued by the Commissioner may also provide practical guidance to data subjects, in particular, the manner in which their personal data privacy right is to be properly protected.

Suggested Amendments

That section 8(5) of the Ordinance be amended to add the words, "and data subjects" after the phrase, "for the guidance of the data users".

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Not recommended for the following reason :

It involves simple clarification only and therefore is unlikely to be controversial to warrant public consultation.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 11

That the Commissioner be conferred with specific power to carry out "preliminary enquiry" for deciding whether to exercise investigation power under section 38 of the Ordinance.

Reasons for the Proposal

1. The Commissioner has discretionary power under section 39(2) of the Ordinance to refuse to carry out or continue with an investigation on specific grounds. Generally, upon receiving a complaint, it is necessary for the Commissioner to carry out preliminary enquiry to gather further information and evidence in order for him to decide whether to carry out an investigation.

2. The Complaint Handling Policy published by the PCPD also expressly states that before the Commissioner invokes his power of investigation under Part VII, preliminary enquiries are normally carried out, which may include mediation, to see whether the case can be resolved without a formal investigation. Moreover, the Commissioner may refuse to carry out or continue with an investigation if after preliminary enquires made by him, there is no *prima facie* evidence of contravention of the requirements of the Ordinance.

3. Although it may be argued that such a power falls within the incidental power under section 8(2) being *"… necessary for, or incidental or conducive to, the better performance…"* of the Commissioner's functions and powers, there is no express power conferred under the Ordinance.

4. The power to conduct preliminary enquiries by the Commissioner was formally challenged and heard in 2 AAB decisions. In AAB No. 11/2004, the Board Chairman made the following findings:-

> *"In our judgment, s.8(2) of the Ordinance empowers the Commissioner to do all such things as are necessary for, or incidental or conducive to, the better performance of his functions and s.39 gives Commissioner wide discretion to refuse*

to carry out an investigation, in particular, he may do so if for any reason an investigation is unnecessary. Under these two sections, the Commissioner may decide in what manner he should perform his functions or exercise any of his powers in respect of a complaint received by him. Thus, to have a preliminary enquiry before exercising his power to decline an investigation is well within the powers conferred on him by the Ordinance provided that he takes into consideration all the circumstances of the case and acts reasonably."

5. In a recent AAB decision No.35/2006, the Deputy Chairman however cast doubts on the power to carry out preliminary enquiry by the Commissioner before an investigation is carried out. The Board states at paragraph 8 of the Decision as follows:-

> "*Suffice for us to observe that we are far from being satisfied that the "preliminary enquiry" made by the Commissioner was made pursuant to some inherent power of the Commissioner not spelt out in the Privacy Ordinance (as opposed to the statutory powers of investigation conferred on him by s.38 of the Privacy Ordinance).*"

6. Reference is made to overseas privacy legislations and enabling legislations of local regulatory bodies for which specific power to conduct preliminary enquiry is found. For instance, section 42 of the Federal Privacy Act of Australia enables the privacy commissioner to make inquiries for the purpose of determining whether he has power to investigate the matter for which the complaint relates or whether he may in his discretion decide not to investigate the matter. In Hong Kong, section 11A of the Ombudsman Ordinance, Cap 397 confers power upon the Ombudsman to carry out preliminary inquiries for determining whether to undertake an investigation.

7. Given the difference in the rulings of the AAB mentioned above and it is essential for the Commissioner to gather information in order to decide whether to exercise his power of investigation, the Commissioner finds it in the interest of certainty that specific power to conduct preliminary enquiry be provided for under the Ordinance.

Suggested Amendment

That a new section 38A be added to provide for specific power of the Commissioner to carry out “preliminary inquiry” for deciding whether to exercise investigation power under section 38.

The Commissioner’s Disposition

Supported.

Public Consultation : Recommended or Not

Not recommended for the following reason :

The specific provision to carry out preliminary inquiries serves no more than to spell out the implied power vested upon the Commissioner. It is a tidying up exercise unlikely to meet public’s disapproval.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 12

That the Commissioner may refuse to carry out or continue with an investigation under section 39(2) where (i) the primary cause of complaint was not related to personal data privacy; (ii) the complaint relates to any action which the complainant has a remedy in court or tribunal or is currently or soon under investigation by another regulatory body; or (iii) 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.

Reasons for the Proposal

1. Although section 39(2)(d) of the Ordinance has apparently provided the Commissioner with a wide discretion to refuse to carry out or continue with an investigation if it is "…for any other reason unnecessary", there are some common situations that the Commissioner will refuse to exercise the power of investigation :

   (i) where the primary cause of the complaint was not related to personal data privacy;

   (ii) where the complaint relates to an action which the complainant has a remedy in any court or tribunal or is currently or soon under investigation by another regulatory body; and

   (iii) where the act or practice specified in the complaint relates to personal data or documents containing personal data which have been or will likely be or intended to be used at any stage in any legal proceedings or inquiry.

2. In situation mentioned in (i) above, complainants have sometimes made use of the redress channel under the Ordinance to vent personal feud or in order to put pressure upon the other party to achieve objective other than genuine concern for protection of his or her personal data privacy right. It is beyond the legislative intent of the Ordinance for the Commissioner to intervene in personal disputes or feuds without further evidence or proof to show how the act or practice would have an impact on personal data

privacy or how it has caused damages or suffering to the data subject concerned. The resources of the Commissioner should be more usefully employed in other worthy cases.

3. As for situations mentioned in (ii) above, the complainant may simultaneously lodge complaint or report the matter to other regulatory or law enforcement agencies for follow up actions. For instance, a complainant may report to police on suspected offence of identity theft. For cases where the effective and more appropriate complaint or redress channel lies with other regulatory bodies, the investigation by the Commissioner on the same matter may prejudice or affect the investigation works undertaken by these regulatory bodies. Sometimes the act or practice complained of, if proved, would constitute an offence, e.g. the offence of forgery under section 71 of the Crimes Ordinance or the offence of computer crime under section 27A of the Telecommunications Ordinance. It has been the policy of the Commissioner to advise the complainant to refer the matter to the police for follow up actions.

4. The Commissioner would also be unlikely to intervene where the proper forum for resolving the dispute in question lies not with the Commissioner but with other redress bodies. For instance, in an AAB case[1], the ex-employee sought to correct the remarks and comments made by his employer in the letter of dismissal by way of making a data correction request under section 22 of the Ordinance. The AAB took the view that in a notice of termination, personal data dealing with the employee's job performance was inherently contentious and it was unlikely that the dismissed employee would share the employer's point of view. The Board opined that the proper venue to resolve such dispute lies with the Labour Tribunal.

5. Reference is also drawn from the provision of section 10(1)(e)(ii) of the Ombudsman Ordinance which provides that the Ombudsman shall not investigate a complaint if it relates to any action of which the complainant has or had "… a remedy by way of proceedings in a court … or in any tribunal constituted by or under any Ordinance".

6. As for situations stated in (iii) above, the common example is where the complainant is engaging in a fishing expedition to obtain documents and data through the lodging of a data access request which he would otherwise only be entitled to under discovery procedures taken in legal proceedings. It has been the view of the Commissioner that a data access

[1] AAB No. 22/2000

request under section 18 of the Ordinance should not be abused to substitute or bypass the proper procedures of discovery made available under proper legal procedures. The view was shared by the Judge in a judicial review application[2] that where the data subject had obtained or could have obtained copies of his personal data through legal proceedings, it would be meaningless and a waste of public funds for him to lodge a complaint with the Commissioner on non-compliance with a data access request and for the Commissioner to investigate the matter. In a recent judicial review application[3] made against the Administrative Appeals Board's decision concerning compliance with a data access request lodged by the Appellant, the Court states in paragraph 34 of the judgment as follows:-

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

7. These are specific grounds that the Commissioner finds it justifiable for their being independently recognized as constituting a ground for refusal under section 39(2) for the following reasons:

(i) It will send out message clear and loud as to the specific circumstances under which the Commissioner will refuse to carry out an investigation; data subjects are therefore better appraised of the situations before lodging a complaint with the Commissioner;

(ii) It saves time and resources for the Commissioner to explain in details why investigation is "for any other reason" unnecessary under section 39(2)(d); and

---

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

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

(iii) Should an appeal be lodged or action be taken against the decision made by the Commissioner, it will facilitates the AAB and the Court to have a more focused approach in deciding whether the discretion of the Commissioner is properly exercised by reliance on these specific grounds for refusal.

Suggested Amendments

That the following subsections be added to section 39(2) to provide for specific grounds of refusal to carry out or continue an investigation initiated by a complaint where having regard to all the circumstances of the case –

(e) the primary cause of complaint was not related to personal data privacy;

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

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

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reason :

As it concerns the grounds upon which Commissioner may refuse to carry out an investigation, it affects the privacy interests of individuals who should be consulted on their inclination and responses.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 13

That the Commissioner may refuse to continue an investigation at any time by giving notice and reasons to the complainant.

Reasons for the Proposal

1. The current provision of section 39(3) prescribes a statutory period of 45 days for the Commissioner to notify the complainant should he refuse to carry out or continue an investigation initiated by a complaint.

2. The Commissioner has encountered practical difficulties in complying with the 45-day period owing to:-

   (i) delay of complainant in providing essential information, such as contact detail, identity proof, consent to disclosure of identity or clarification of the complaint points which hinder the work progress of the Commissioner; and

   (ii) delay of the party complained against to provide responses owing to time and efforts needed to retrieve relevant information and supply evidence or seek legal advice before responding.

3. The Commissioner had tried to trace the rationale at the legislative stage for the imposition of the 45-day period under section 39(3). There does not appear to have been any discussion on the reasons for such imposition by the then Bills Committee. Both the Law Draftsman and the Home Affairs Bureau (the then responsible policy bureau) were consulted and they confirmed that there was no record of discussion on the subject matter.

4. The Commissioner has also studied respective ordinances of other local regulatory bodies (such as the Ombudsman and the Equal Opportunities Commission) as well as overseas privacy legislations but could not find any similar approach in prescribing time limit for the regulatory body to notify the complainant of refusal to carry out or continue an investigation. A guess of the intention behind is that it is in accordance with the principle

of good governance.

5. The Commissioner fully supports the principle of good governance that when he decides not to carry out an investigation, he should as soon as practicable notify the complainant of the same and the reasons.

6. However, where the Commissioner has commenced an investigation and matters surfaced subsequently which he finds it justifiable and reasonable to discontinue the investigation, he is not empowered under the current provision of the Ordinance to do so after expiration of the 45 days. He is bound to continue with an investigation even if he discovers that the complaint was not made in good faith (section 39(2)(c) refusal ground) or that the party complained against has already taken remedial action and the dispute considered resolved and hence further investigation is considered unnecessary (section 39(2)(d) refusal ground).

7. For reason of fairness to the party complained against and proper utilization of resources, the Commissioner finds it desirable that the time limit imposed under section 39(3) does not apply to a decision to discontinue an investigation.

Suggested Amendments

That the following amendments be made to section 39:-

(a) in subsection (3), by repealing "or continue" after "carry out";

(b) by adding the following immediately after subsection (3):-
"(3A) Where the Commissioner refuses under this section to continue an investigation initiated by a complaint, he shall by notice in writing serve on the complainant accompanied by a copy of subsection (4), inform the complainant—
(a) of the refusal; and
(b) of the reasons for the refusal."

(c) In subsection (4)(a), by adding "or subsection (3A)" after "subsection (3)."

Following the creation of a new subsection (3A) of section 39, an appeal right should be given to the complainant where a refusal is made under the new subsection. Consequential amendments therefore have to be made to the Administrative Appeals Board Ordinance (Cap. 442) under item 29 "Personal

Data (Privacy) Ordinance" in the Schedule—

(a) in paragraph (c), by repealing "or continue" after "carrying out" and

(b) by adding the following immediately after paragraph (c):-
"(ca) to refuse under section 39(3A) to continue an investigation initiated by a complaint."

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reason :

As it concerns the powers of the Commissioner to discontinue an investigation at any time during the course of an investigation, it affects the privacy interests of the complainants and as such public scrutiny is needed.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 14

That the Commissioner may call upon public officers to assist him in the performance of his regulatory function under the Ordinance.

Reasons for the Proposal

1. In exercise of the Commissioner's powers of investigation and inspection, the Commissioner may exercise such ancillary powers as making entry into premises (section 42(2) refers). When resistance or obstruction is encountered, it may give rise to the need to seek assistance from the police.

2. Expert advice and assistance are also required in investigation entailing :

   (i) information technology and computer forensics (e.g. digital evidence search, internet traces and log analysis);

   (ii) identification of suspects by use of digital images; and

   (iii) reconstruction of criminal activities requiring software analysis, reverse engineering, decryption and presentation of digital data.

3. Expert assistance of the sort mentioned above is particularly relevant when the Commissioner is conferred with power to investigate offence and to institute prosecution. The help from other public officers, such as the Police, Government Laboratory, etc. for evidence gathering purpose and identifying the data subject or the culprit in question is of immense value. It will also save time and costs in retaining experts outside the Government.

4. To facilitate the better performance of the Commissioner's regulatory functions under the Ordinance, it is necessary to confer on him an express power to request assistance from public officers, rather than relying on the goodwill of these public officers to render assistance.

5. Reference was drawn from the Unsolicited Electronic Messages Ordinance

for which a similar power is conferred[1] on the Telecommunications Authority to solicit assistance from public officers for the purpose of investigation.

Suggested Amendment

That section 43 be amended to incorporate an express power for the Commissioner to call upon public officers to assist.

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Not recommended for the following reason :

It is a proposal to enhance the efficient discharge of the investigative power of the Commissioner and will likely gain public support.

[1] See section 40(5) of the Unsolicited Electronic Messages Ordinance which provides "the Authority or an authorized officer may call upon police officers or other public officers to assist him in the performance of any function under this section". http://www.legislation.gov.hk/blis_pdf.nsf/6799165D2FEE3FA94825755E0033E532/BE5AA57E2A0358C7482575EF00201941/$FILE/CAP_593_e_b5.pdf

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 15

To confer power upon the Commissioner to conduct hearing in public unless he is of the opinion that the hearing should be carried out in private having regard to all the circumstances of the case including written request from the complainant.

Reasons for the Proposal

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

2. The Commissioner finds the provision too restrictive that hinders him from holding the hearing in public, particularly when issues of public interest and importance are involved and when members of the public have a genuine right to know and to be informed.

3. Moreover, an investigation may involve more than one complainant or affect more than one data subject. It may not be in the public interest or in the interest of other complainants or data subjects to have a private hearing if only one or a small number of complainants object to hold the hearing in public.

4. It is therefore proposed that the Commissioner shall decide whether hearing should be held in public having regard to all the circumstances of the case including any request made by a complainant.

Suggested Amendment

That section 43(2) be replaced by the following:-

"Any hearing for the purposes of an investigation shall be carried out in public

unless the Commissioner is of the opinion that the investigation should be carried out in private after considering all the circumstances of the case including, if the investigation was initiated by a complainant, any written request from the complainant that the investigation be carried out in private."

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Not recommended for the following reason :

A minor amendment which does not affect public interest.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 16

To confer power upon the Commissioner and his prescribed officers to search and seize evidence in the exercise of his regulatory functions under the Ordinance.

Reasons for the Proposal

1. At present, the Commissioner is equipped with the following power to carry out investigation:-

   (a) power to be furnished with any information, document or thing from any person (s.43);
   (b) power to enter premises (s.42);
   (c) power to summon witnesses (s.44); and
   (d) power to conduct hearing (s.43).

2. There is, however, no power vested upon the Commissioner to search and seize evidence. Essential or important pieces of evidence, such as computers and diskettes, etc. may have been concealed or dissipated. In order to carry out criminal investigation, it is necessary for the Commissioner to be equipped with the power to search and seize evidence in order to gather evidence for prosecution proceedings.

3. As a measure to ensure the proper exercise of this power, criteria may be laid down which are to be satisfied :-

   (a) the Commissioner reasonably believes that there is any property or document that contains evidence which may be required in the proceedings for an offence under the Ordinance;

   (b) the offence was, has been or is about to be committed; and

   (c) the property or document is likely to be of value to any investigation into such offence.

4. As a further safeguard against possible abuse of power, a warrant has to be

obtained from the Magistrate authorizing the Commissioner to exercise such power.

5. Reference was made to the similar power being conferred on the Telecommunications Authority under the Unsolicited Electronic Messages Ordinance[1] to facilitate investigation with the ultimate goal of bringing prosecution.

Suggested Amendment

That section 42 be amended to confer on the Commissioner the power to search, seize, remove and detain property and documents upon issuance of a warrant by a Magistrate.

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reason :

It concerns increase of the Commissioner's investigation power and hence public scrutiny and feedbacks should be sought.

[1] See sections 40 and 41 of the Unsolicited Electronic Messages Ordinance http://www.legislation.gov.hk/blis_pdf.nsf/6799165D2FEE3FA94825755E0033E532/BE5AA57E2A0358C7482575EF00201941/$FILE/CAP_593_e_b5.pdf.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 17

The time limit for laying information for prosecuting an offence under the Ordinance shall be two years from commission of the offence.

Reasons for the Proposal

1. The statutory time limit for laying information to prosecute an offence under the Ordinance is prescribed under section 26 of the Magistrates Ordinance. The provision states that information shall be laid before a magistrate within six months of commission of the offence. In the Commissioner's experience, the period of six months is insufficient because of the following reasons:-

   (i) The parties and witnesses may not be cooperative in furnishing relevant information which has a direct bearing on the time to be spent for making inquiries and gathering of evidence by the Commissioner;

   (ii) The time required by the Commissioner to analyse technical issues of the case (e.g. where complex technologies are involved), the proper application of the relevant provision of the Ordinance, the need to obtain legal advice in assessing the weight and relevancy of the evidence, etc;

   (iii) The time that Police has to spend in carrying out investigation on a suspected offence referred by the Commissioner; and

   (iv) According to the Secretary of Justice, at least two months' time should be allowed for the provision of legal advice and the initiation of prosecution proceedings.

2. Practical difficulties were encountered in a case referred by the Commissioner to the police for prosecution on non-compliance of an enforcement notice issued by the Commissioner. In that case, the relevant data user lodged an appeal with the Administrative Appeals Board against the issuance of the enforcement notice. The appeal was

subsequently dismissed by the Board. The police, upon legal advice, found it difficult to determine the date of commission of the offence and advised against prosecution. The issue of whether the offence in question was a single or continuous offence was raised, as it would have bearing on counting the six months' time bar period. It was only after several exchanges of legal views that the Department of Justice was finally convinced that it was within time for prosecution of the case.

3. The above demonstrates the harshness of the six months' period prescribed under section 26 of the Magistrates Ordinance when prosecution is brought under the Ordinance. In order that prosecution of offences not to become stale by exceeding the statutory time limit, it is proposed that the appropriate time for laying information before a Magistrate be set for two years after commission of an offence. The period is consistent with the spirit of section 39(1)(a) of the Ordinance which provides that the Commissioner may refuse to carry out an investigation initiated by a complaint if the complainant had actual knowledge of the act or practice specified in the complaint for more than two years immediately before the lodgment of the complaint.

Suggested Amendment

That the statutory time limit for laying information for prosecution of an offence under the Ordinance be set at two years after commission of the offence.

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reason:-

Since the proposed time limit of two years has exceeded the current time limit of six months prescribed under section 26 of the Magistrate Ordinance, responses from the public on the justifications put forward by the Commissioner under the proposal should be sought.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 18

That the Commissioner and his prescribed officers shall be immune from suit for any act done or omission made in good faith in the exercise or purported exercise of his functions and powers under the Ordinance.

Reasons for the Proposal

1. In order that the Commissioner can perform his regulatory functions without fear, it is essential that he should be immune from suit for actions brought against him as a result of the exercise of his functions and powers under the Ordinance. Such immunity shall be granted to the Commissioner in his personal capacity and to the prescribed officers appointed by him under the Ordinance.

2. It is not uncommon that immunity is conferred upon the regulators performing functions similar to the Commissioner. For instance, section 18A of the Ombudsman Ordinance grants immunity to protect any persons acting in good faith from personal liability for any civil liability or claim in respect of act done or omitted to be done in the performance or purported performance of the functions and the exercise of the powers conferred under the Ombudsman Ordinance. Similar protections are found under section 45 of the Unsolicited Electronic Messages Ordinance and section 42B of the Mandatory Provident Fund Schemes Ordinance.

3. Since the Commissioner and the individual prescribed officers appointed by him may be named as parties or co-defendants in a law suit, the immunity now proposed is imperative in providing a good defence to an action filed against the Commissioner and/or his prescribed officers.

Suggested Amendment

That the Commissioner and his prescribed officers shall be protected from suit for any act done or omitted to be done by him or his prescribed officers in good faith in the exercise or purported exercise of the functions and powers under the Ordinance.

The Commissioner’s Disposition

Supported.

Public Consultation : Recommended or Not

Not recommended for the following reason :

It is unlikely to be an issue of controversy given that statutory immunity is conferred on other regulatory bodies performing statutory functions.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 19

That wider discretion be conferred on the Commissioner to decide whether to issue an enforcement notice under section 50, having due regard to certain factors. The enforcement notice may contain direction requiring the relevant data user to desist from doing an act or engaging in a practice.

Reasons for the Proposal

1. Under the current section 50, one of the following criteria has to be met before the Commissioner will issue an enforcement notice, namely –
   (a) that the data user is contravening a requirement under the Ordinance (section 50(1)(a)); or
   (b) that the data user has contravened such a requirement in circumstances that make it likely that the contravention will continue or be repeated (section 50(1)(b)).

2. Besides, pursuant to section 50(2), the Commissioner shall consider the damage or distress that the contravention has caused or is likely to cause to the data subject. The section, however, does not stand alone to constitute an independent factor that can be taken into account by the Commissioner without reference to the criteria laid down in section 50(1) and no such legislative intention could be read or implied. The Commissioner cannot issue an enforcement notice if the act or practice has ceased without information to show likelihood of repetition, though the harm or damage caused or the impact on personal data privacy is significant.

3. A study on overseas privacy legislations shows that where enforcement power is conferred, no such condition similar to those found in section 50(1) of the Ordinance is imposed. All that the privacy commissioner overseas need to consider is whether the contravention has caused or is likely to cause any person damage or distress[1].

4. Hence, the Commissioner finds the provisions overly restrictive to hinder the issuance of an enforcement action. The Commissioner considers it

[1] See e.g. section 40 of the UK Data Privacy Act 1998 http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_6#pt5-l1g40.

more effective if discretion is given to him for issuance of enforcement notice to rectify the wrongful act insofar as he has given due regard to the following factors:-

(i) whether the act of contravention is continuing;

(ii) whether the contravention will continue or be repeated;

(iii) whether the contravention has caused or is likely to cause any harm to the data subject; and

(iv) such other matters as the Commissioner may think fit to consider.

5. The Commissioner also noted that in issuing an enforcement notice, he is required under section 50(1)(iii) to specify a period within which the remedial steps are required to be taken by the data user. The prescribing of a period for certain act or practice to cease may be ill conceived by the data user to apply to the period specified only but not thereafter. On the other hand, by specifying that the remedy is to last after expiration of the specified period is arguably ultra vires the powers of the Commissioner under section 50(1)(iii).

6. In order to mend the legislative loophole, the Commissioner proposes that explicit power be conferred under section 50(1) for the Commissioner to direct the relevant data user in the enforcement notice to desist from doing an act or engaging in a practice in order to quell any doubt on the power of the Commissioner.

Suggested Amendments

(A) That subsection (1) of section 50 be repealed and substituted by the following:-

"Where, following the completion of an investigation, the Commissioner is of the opinion that the relevant data user has contravened a requirement under this Ordinance and that it is appropriate to do so after taking into account the following matters:-

(a) whether the contravention of any requirement under this Ordinance is continuing;

(b) whether the contravention of any requirement under this Ordinance will continue or be repeated;

(c) whether the contravention or matter relating to the contravention has caused or is likely to cause damage or distress to any individual who is the data subject of any personal data to which the contravention or matter as the case

may be relates; and

(d) any other matters as the Commissioner may think fit to consider

then the Commissioner may serve on the relevant data user a notice in writing:-

(i) stating that he is of that opinion;

(ii) specifying the requirement as to which he is of that opinion and the reasons why he is of that opinion;

(iii) directing the data user to take such steps or to cease such act or practice as are specified in the notice to remedy the contravention or, as the case may be, the matter occasioning it within such period (ending not earlier than the period specified in subsection (7) within which an appeal against the notice may be made) as is specified in the notice; and

(iv) accompanied by a copy of this section.

(B) That subsection (2) of section 50 be repealed.

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reason :

As a result of the amendment, more data users will be caught as a result and it is therefore a matter of public interest that should be included for public consultation.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 20

To enable a data user to refuse compliance of a data access request made by a requestor "on behalf of" a minor as relevant person if the data user has reasonable ground for believing that compliance is contrary to the minor's interests.

Reasons for the Proposal

1. Section 18(1) of the Ordinance provides that an individual **or a relevant person** on behalf of an individual may make a data access request to the data user in respect of personal data of which the individual is the data subject. The meaning of "relevant person" is defined under section 2(1) of the Ordinance as including "where the individual is a minor, a person who has parental responsibility for the minor".

2. Question arises as to whether a parent is in fact making a data access request as relevant person **on behalf of** his or her minor child particularly when the data subject himself has expressed disagreement to such disclosure or where the relevant person is not in fact making the request "on behalf of" the minor. A typical example is the case where the estranged parent makes a data access request to, for example, the school, the social welfare organizations or Immigration Department for the location data of the child. It is obvious that it is an attempt of the requestor to trace the whereabouts of the child in order to make contact, etc.

3. The situation is unsatisfactory as the parent may access and obtain the personal data of his or her minor child as "relevant person" under a data access request made under section 18. Since protection of the minors is of prime concern to any legislator, the definition of "relevant person" should be reviewed to obviate the anomaly created by a parent who abuses the access mechanism to obtain personal data of the child for his or her own purpose rather than making it "on behalf of" the child. Public interest also dictates that personal data of the child should not be easily obtained by a parent who is suspected to have committed child abuse on his or her minor child to protect the child from further molestation and for protection

of the child's physical and mental health.

4. Overseas privacy legislations have been examined. In New Zealand, section 29(1)(d) of the Privacy Act 1993 provides a ground for refusal to disclose personal information of an individual under the age of 16 if it would be contrary to the individual's interest. In UK, there is no similar provision on a parent acting as relevant person of the minor to make a data access request. Instead, section 66 of the UK Data Protection Act 1998 has specified the test on ascertaining the legal capacity of a person under the age of 16 (and above the age of 12) to exercise his data privacy right. According to that section, the person shall be taken to have that capacity where *"he has a general understanding of what it means to exercise that right"*.

5. To address the unsatisfactory situation, the Commissioner considers that data users should in appropriate cases be able to refuse to comply with a data access request made by a requestor purportedly on behalf of a minor as the relevant person. In the Commissioner's view, there are two ways to achieve this end:-

   (1) Firstly, the data user may refuse to comply with such a data access request if justified by the data user's reasonable belief. To this end, a new subsection 20(3)(ba) may be inserted immediately after section 20(3)(b) to the following effect:-

   > "*(ba) the request is made by a requestor on behalf of a minor as relevant person and the data user has reasonable grounds for believing that:-*
   >
   > *(i) the minor gave the requested personal data to the data user on the explicit understanding that they would not be disclosed to the requestor;*
   >
   > *(ii) the minor is a victim of child abuse and the requestor is a suspected perpetrator; or*
   >
   > *(iii) the parents of the minor are divorced or separated, and the requestor does not have custody of the minor.*"

   (2) Alternatively, a general ground can be introduced based on section 29(1)(d) of the New Zealand Privacy Act 1993. In this connection, the new subsection 20(3)(ba) should be inserted immediately after

section 20(3)(b) to the following effect:-

> "*(ba) the request is made by a requestor on behalf of a minor as relevant person and the data user has reasonable grounds for believing that compliance with the request would be contrary to the interests of the minor.*"

6. The Commissioner considers that the proposal modeling on New Zealand Privacy Act as set out in paragraph 5(2) above is preferred because it provides more flexibility in accommodating different situations.

Suggested Amendments

To insert a new subsection 20(3)(ba) immediately after section 20(3)(b) to the following effect:-

> "*(ba) the request is made by a requestor on behalf of a minor as relevant person and the data user has reasonable grounds for believing that compliance with the request would be contrary to the interests of the minor.*"

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reasons :

The responses from previous consultation conducted by the Home Affairs Bureau indicated a diverse in opinions as to what age a minor should attain before a parent is prevented from exercising the right as "relevant person" to access the personal data of his child. This leads to the further question as to whether a minor has the mental capacity to give "prescribed consent" for handling of his or her personal data.

In view of the significant impact that the amendments will limit the scope of parental right to access personal data of the minor child and the need to give sufficient childcare protection, the proposal shall be put forward for public

consultation.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 21

To impose an explicit duty on the data user to respond to a data access request within the statutory period of 40 days even though the data user does not hold the requested data.

Reasons for the Proposal

1. Two distinctive requests can be made by a data subject to a data user under section 18(1) of the Ordinance, namely, (i) to be informed whether the data user holds his personal data (section 18(1)(a)); and (ii) if the data user holds such data, to be supplied with a copy of such data (section 18(1)(b)). Section 18(3) provides that a data access request made under section 18(1)(a) may, in the absence of evidence to the contrary, be treated as a data access request made under both (i) and (ii). However, the reverse situation is not provided for under section 18(3).

2. Hence, where a requestor has made clear in the data access request for section 18(1)(b) alone (i.e. to be supplied with a copy of the data) and the data user in fact does not hold the personal data, it can be logically argued that there is nothing in the request for the data user to comply with. It then follows that the obligation of the data user to respond within 40 days under section 19(1) to comply with the data access request does not arise.

3. The result is that the requestor will be kept in the dark as to the reason for not responding by the data user. Complaints will be filed by the requestor to the Commissioner on the suspected non-compliance of the data access request by the data user.

4. This has become the bone of contention in AAB No. 43/2004. The complainant indicated in his data access request form that the request was made under section 18(1)(b) only. Since the data user did not hold or possess the requested data, no reply was furnished to the requestor within 40 days. The Commissioner was of the view that there was no contravention of the Ordinance. In dismissing the appeal, the Board stated that where a data access request was made under section 18(1)(b) alone, it would be against the legislative intent of the Ordinance that the

data user was thereby under no duty to respond to the requestor within 40 days the fact that it did not hold the data. However, given that contravention of the data access request provisions under the Ordinance would constitute an offence, the Board was doubtful as to whether there was contravention and therefore could not say that the decision of the Commissioner was wrong.

5. In order to cure this unsatisfactory situation, the Ordinance should be amended to impose an explicit duty or otherwise to make known clearly to the data subject that the data access request would not and could not be complied with.

Suggested Amendment

That section 19 of the Ordinance be amended to impose a duty upon the data user to respond within 40 days of receipt of the data access request even though there is no personal data of the data subject held by it. Alternatively, section 20 may be amended to make it a valid ground for refusal to comply with a data access request if the data user does not hold the personal data in question.

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Not recommended for the following reason :

This is a technical amendment with no adverse impact on personal data privacy. The proposed amendment is unlikely to be objected by the general public.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 22

To provide for a new ground of refusal to comply with a data access request on the basis of self-incrimination.

Reasons for the Proposal

1. An individual has the fundamental right and privilege against disclosure of any information or data that may incriminate him.

2. The Ordinance does not contain any provision abrogating this common law right and it would be against the legislative intent of the Ordinance that such common law right be affected. Hence, a data access request should not be used as an instrument to obtain information which is self-incriminating against the data user. The principle of privilege against self-incrimination should be upheld.

3. Notwithstanding the aforesaid, the Ordinance as it currently stands does not provide that compliance of a data access request will incriminate the data user as a valid ground for refusal to comply with the data access request. Nor is there a specific exemption provision under Part VIII of the Ordinance exempting from the application of DPP6 and section 18(1)(b) where compliance of the same will prejudice the common law privilege against self-incrimination.

4. Reference was made to paragraph 11 of Schedule 1 of the UK Data Protection Act 1998 which provides that *"a person need not comply with any request or order under section 7 to the extent that compliance would, by revealing evidence of the commission of any offence other than an offence under this Act, expose him to proceedings for that offence"*. Information so disclosed is not admissible as evidence against him in proceedings of an offence brought under the Act.

Suggested Amendment

That an additional exemption from compliance with a data access request be

provided for where the compliance of the request would, by revealing evidence of the commission of any offence other than an offence under the Ordinance, expose the data user to proceedings for that offence.

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Not recommended for the following reason:

This is consistent with the common law principle of privilege against self-incrimination which is to be respected and upheld by all legislators. No controversy of public opinions is anticipated.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 23

To provide for a new ground of refusal to comply with a data access request where the data user is obliged or entitled under any other statutory provisions not to disclose the personal data in question.

Reasons for the Proposal

1. The duty to comply with a data access request has been challenged in situation where there co-exists a statutory duty of secrecy on the part of the data user not to disclose any information held by it or came to its knowledge. Compliance with the data access request would mean a breach of the statutory duty of confidence or secrecy which very often carries with it penal consequences. Some data users argued that this should be accepted as a valid ground for non-compliance with the data access request.

2. However, since the statutory duty to maintain secrecy is neither recognized nor provided for under section 20(3) of the Ordinance as a ground of refusal to comply with a data access request, the Commissioner cannot accept the argument put forward as constituting a valid ground of refusal.

3. It is worthy to note that the Ordinance does not contain any provision that gives it an overriding effect over any other ordinances in case where there are conflicting provisions. It has become an academic question as to whether any subsequent legislation (i.e. legislations enacted after the coming into being of the Ordinance) which contains a secrecy provision should be viewed as having the legal effect of implied repeal of the parts of the Ordinance which are inconsistent so that it would afford a good ground of refusal to comply with a data access request made under section 18 of the Ordinance.

4. It is undesirable that compliance with the data access request may induce a breach of the statutory duty of secrecy owed by a data user. It is also unfair to the data user that he/she is facing a dilemma of breaching either the data access request provision under the Ordinance or the secrecy provisions in another ordinance. Having regard to the legislative intent

for maintaining secrecy under various ordinances, the Commissioner proposes that it be made a specific ground for which a data user may rely upon to refuse to comply with a data access request.

Suggested Amendment

That section 20(3) of the Ordinance be amended to provide for a new ground to refuse compliance with a data access request in relation to personal data which the data user is obliged or entitled under any ordinances not to disclose.

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reason :

Since it affects or to some extent deprives the data subject's right to access his personal data conferred under the Ordinance and it also leads to the further issue as to whether the exemption should also extend to a data user who owes a duty of secrecy under contract or by virtue of professional relationship, the matter merits public consultation.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 24

To amend section 20(2) of the Ordinance to make easier reading and facilitate understanding in respect of the duty to comply with a data access request without disclosing personal data of which other individual is the data subject.

Reasons for the Proposal

1. Section 20(1)(b) and 20(2) contain provision protecting personal data of other individuals from being disclosed when a data user complies with a data access request. In essence, unless with the consent of that other individual, his names or other identifying particulars should be omitted.

2. A typical example is found in a data access request for a staff's appraisal report. According to section 20(1)(b) and (2), the data user is only obliged to edit out the names, job titles, etc. of the appraising officer or other persons having given comments about the appraisee although the requestor may somehow be able to know their identities, e.g. from the contents of the appraisal or the requestor's personal knowledge.

3. In considering whether third parties' personal data are adequately protected under section 20(2)(a) and (b), reference has been made to overseas privacy legislations.

4. In the UK, the Data Protection Act has taken a more liberal approach in recognizing the situation that personal data of third parties may be disclosed without their consent if it is reasonable in all the circumstances of the case for the data controller to do so.

5. In Canada, section 9 of the Personal Information Protection and Electronic Documents Act provides that unless with the consent of third party, an organization shall not give an individual access to personal information if doing so would likely reveal personal information about a third party. However, if information about the third party is severable from the record containing the information about the individual, the organization shall sever such information about the third party.

6. In Australia, the National Privacy Principle 6.1 of the Privacy Act 1988 enables access to personal information except where it would have an unreasonable impact upon the privacy of other individuals.

7. The privacy legislation in New Zealand confers a wide power upon the data user to withhold information insofar as "there is good reason for withholding some of the information contained in that document". Such good reason may include where disclosure would involve the unwarranted disclosure of the affairs of another individual or where it discloses the third party as source of the evaluative material held in confidence by the data user.

8. Thus, it can be seen that different privacy legislations have adopted a range of approaches in handling personal data of third parties from merely deleting the names and identifying particulars to the deletion of more information when it is reasonable to do so.

9. Section 20(1)(b) and 20(2) as it currently stands has struck a fair balance by requiring only the deletion of names and identifying particulars of third parties without imposing onerous burden upon the data user.

10. Hence, without the need to call for substantial amendments, the drafting of section 20(2) can be improved in order to achieve easier understanding and reading by members of the public.

Suggested Amendment

That sub-paragraphs (a) and (b) of section 20(2) of the Ordinance be deleted and replaced by the following:-

"(a) Subsection (1)(b) shall not operate to excuse a data user from complying with the data access request concerned to the extent that the request may be complied with without disclosing the identity of the other individual, whether by the omission of names, or other identifying particulars, or otherwise.

(b) Where personal data being requested contain information identifying another individual as the source of the data, the prohibition against disclosure of another individual's personal data imposed by subsection (1)(b) shall extend only to such information that names or otherwise

explicitly identifies him."

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Not recommended for the following reason :

This is only an improvement on the drafting without proposing substantial change to the approach in dealing with third parties' personal data when complying with a data access request. As such, there is no need to have the proposal included for public consultation.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 25

Personal data being sought in a data access request, which is in dispute, should not be disclosed to the data requestor until determination by the Administrative Appeals Board or the Court in favour of the data subject.

Reasons for the Proposal

1. The bone of contention of a complaint about non-compliance with data access request ("DAR") usually involves the non-supply or excessive redaction of the requested data. In the course of enquiry or investigation, the Commissioner will often request production of the documents in dispute for inspection before arriving at his finding. The decision of the Commissioner is subject to appeal to the Administrative Appeals Board ("AAB")[1]. An aggrieved party may also seek other legal remedies, such as by applying for judicial review.

2. When the administrative appeal procedure is engaged, save for documents for which a claim to privilege against disclosure is made, the Commissioner is obliged to give description of every document that is in his possession or under his control which relates to the appeal[2]. It has been the standing instruction of the AAB that copies of these documents shall be furnished to the appellant and party bound by the decision. Specific right to inspect the documents is also conferred under section 13 of the Administrative Appeals Board Ordinance, Cap. 442. A similar right to discovery of documents is also available when legal action is commenced by the aggrieved party.

3. An anomaly occurs since the documents in dispute (if so possessed by the Commissioner) will be disclosed to the complainant before the hearing of the AAB takes place where the core issue of the appeal is whether the

---

[1] Appeal to the AAB may be brought under sections 39(4) http://www.pcpd.org.hk/english/ordinance/section_48.html or 47(4) http://www.pcpd.org.hk/english/ordinance/section_56.html of the Ordinance by the complainant or under section 50(7) http://www.pcpd.org.hk/english/ordinance/section_59.html by the relevant data user.

[2] Section 11(2)(b) of the Administrative Appeals Board Ordinance http://www.legislation.gov.hk/blis_pdf.nsf/6799165D2FEE3FA94825755E0033E532/26F36CA2A2223F29482575EF000862BE/$FILE/CAP_442_e_b5.pdf.

complainant is entitled to have access to those documents by DAR. It leads to the illogical result that even if the AAB at the end of the day rules in favour of the relevant data user against disclosure, the documents in dispute will nonetheless already have been obtained by the complainant and it renders the appeal hearing otiose.

4. In a recent AAB appeal, such procedure was challenged by the relevant data user in an application for an order to exclude certain documents which are the subject of the DAR from the list of documents to be disclosed to the complainant. The Board refused the application on grounds that (i) the disclosure conforms with the principle of open justice, (ii) there is no provision in the Ordinance prohibiting production of particular documents for the purpose of appeal; and (iii) although section 7 of the UK Data Protection Act 1998 is similar to section 18 of the Ordinance insofar as a data access request is concerned, there is no similar provisions under the Ordinance as in section 15(2) of the 1998 Act prohibiting disclosure of the documents until the question is determined by the court.

5. The Board further states:-

"If this procedure is considered to be unsatisfactory that a data subject may by way of an appeal to the Board gain access to documents which he otherwise would not be able to obtain and may thereby affect the operation of the PDPO, it would be a matter of (personal data privacy) policy for the administration to consider ways to avoid this outcome."

6. The dire consequence is that an individual may seek to access certain documents by way of DAR by abusing the complaint and appeal channels provided under the Ordinance. It is therefore advisable to undergo legislative amendment to close the loophole by building in a provision that personal data being sought in a DAR is not to be disclosed to the complainant until the AAB or the court makes decision in favour of the complainant.

Suggested Amendment

That a new sub-clause (5) shall be added to section 20 as follows:-

"(5) For the purpose of determining any question whether a data user shall or may refuse to comply with a data access request lodged by a requestor (including any question whether any relevant personal data are

exempt from being accessed by virtue of Part VIII), a specified body may require the relevant personal data sought by the requestor to be made available for its own inspection but shall not, pending the determination of that question in favour of the requestor, require the relevant personal data to be disclosed to the requestor whether by discovery or otherwise. For the purpose of this subsection, the term, "specified body" shall have the same meaning as provided under section 13(4) of this Ordinance."

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended in view of the impact that the proposed amendments may have on the general principle of discovery applicable to legal procedures.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 26

To introduce a fees schedule for compliance with data access requests.

Reasons for the Proposal

1. Section 28(2) of the Ordinance provides that a data user may impose a fee for complying a data access request ("DAR") subject to the condition that the fee must not be excessive[1].

2. The ability of an individual to gain access to his personal data is critical to the exercise of his other rights under the Ordinance. Therefore, the fee to be imposed for compliance with a DAR should not be of a level that may deter an individual from making a request.

3. The Ordinance does not define the meaning of "excessive". The fee for supplying a copy of the requested data in a DAR varies considerably from one data user to another. This disparity may be due to the difference in the operation costs of different data users.

4. Throughout the years, the Commissioner's Office has received a number of complaints alleging the imposition of excessive fees by data users for compliance with DARs. Many of these involved only trivial sums. In handling the complaints, the Commissioner's Office has to go into details the composition of the fee as well as its calculation in order to assess whether the fee imposed is excessive. Disproportionate manpower resources are spent in handling the complaints.

5. In addition, some data users reflect that under the current mechanism they have in place, it takes some considerable time and effort for them to locate and retrieve the requested personal data before any payment of fee is made. If the requestor should fail to pay the fee, the manpower cost will be wasted and there is no recourse against the requestor. Prescribing a fees schedule will enable a data user to impose a fee in accordance with the schedule before commencing the process of locating and retrieving the requested data. Unless the DAR fee is paid, no work needs to be carried

[1] Section 28(3), Personal Data (Privacy) Ordinance http://www.pcpd.org.hk/english/ordinance/section_28.html

out by a data user.

6. Currently, the Commissioner will take into account the following criteria in assessing whether a DAR fee is excessive:

   (a) A data user is only allowed to recover *labour costs* and *actual out-of-pocket expenses* involved in the process of complying with the DAR insofar as they relate to the location, retrieval and reproduction of the requested data; and

   (b) The *labour costs* should only refer to the normal salary of a clerical or administrative staff who are able to handle the location, retrieval or reproduction work.

7. A jurisdictional study on overseas privacy legislations on DAR fee has been conducted.

8. In UK, the Data Protection Act 1998 provides that a data controller is not obliged to supply any information unless he has received, except in prescribed cases, such fee (not exceeding the prescribed maximum) as he may require[2]. The prescribed maximum is set at £10 and there are special rules that apply to fees on a request for access to credit reference record (£2), manual health record (£50) and education record (a sliding scale ranging from £1 to £50)[3]. The data user must comply with the request for access by supplying the data subject with a copy of the information unless he can prove "the supply of such a copy is not possible or would involve disproportionate effort"[4]. However, there is no definition of "disproportionate effort" in the Act[5].

9. In Canada, an organization shall respond to an individual's request within

---

2 Section 7(2) Data Protection Act 1998 http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_3#pt2-l1g7

3 Regulation 3, The Data Protection (Subject Access) (Fees and Miscellaneous Provisions) Regulations 2000 SI 2000 No.191 http://www.opsi.gov.uk/si/si2000/20000191.htm

4 Section 8(2) Data Protection Act 1998 http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_3#pt2-l1g8

5 Nevertheless, the Information Commissioner's Office in its information sheet, "How to access your information" provided the following factors to consider the term "disproportionate effort": (a) costs of giving the information; (b) length of time; (c) the difficulty; (d) the size of the organization; and (e) the effect of not providing the information http://www.ico.gov.uk/upload/documents/library/data_protection/introductory/subject_access_rights.pdf

a reasonable time and *at minimal or no cost* to the individual[6]. The organization may respond to an individual's request at a cost to the individual only if the organization has informed the individual of the approximate cost and the individual has advised the organization that the request is not being withdrawn[7]. In practice, the Commissioner will allow the organization to charge a reasonable photocopying fee. The Commissioner will not approve any flat fee that could have the effect of dissuading an individual from making a request[8].

10. In France, a data controller may only require payment of a sum of money not exceeding the costs of complying the access request from a data subject[9].

11. The Australian's statute in this respect is similar to Hong Kong. Principle 6.4 of the Australian Federal Privacy Act 1988 provides "*If an organization charges for providing access to personal information, those charges (a) must not be excessive; and (b) must not apply to lodging a request for access.*"

12. The Australian Privacy Commissioner published Information Sheets to provide guidance to private sector on the fee for access[10]. In summary, the Australian Privacy Commissioner considers a reasonable fee may include:-

    (a) reasonable costs of resources (such as photocopying or reproducing records in other forms);
    (b) reasonable costs for time and labour performed by clerical staff; and
    (c) if necessary, reasonable costs involved in having someone explain information to an individual.

13. In the Australian's model, there is no fee schedule setting out the various fees for access. The Australian Privacy Commissioner in a Complaint

---

6 Principle 4.9.4, Schedule 1, Personal Information Protection and Electronic Documents Act ("PIPEDA") http://www2.parl.gc.ca/HousePublications/Publication.aspx?pub=bill&doc=C-6&parl=36&ses=2&language=E&File=163

7 Paragraphs 8(6)(a) and (b) of PIPEDA http://www2.parl.gc.ca/HousePublications/Publication.aspx?pub=bill&doc=C-6&parl=36&ses=2&language=E&File=47

8 PIPEDA Case Summary #391 http://www.privcom.gc.ca/cf-dc/2008/391_20080225_e.cfm

9 Article 39 Act n° 78-17 of January 1978 on Data Processing, Data Files and Individual Liberties

10 Private Sector Information Sheet 22 – Fees for Access to Health Information under the Privacy Act http://www.privacy.gov.au/publications/IS22_08.pdf and Private Sector Information Sheet 4 – 2001 Access and Correction

Determination considered that the setting of a maximum cost by an organization might be an effective way in avoiding the imposition of an excessive charge for access[11].

14. The Commissioner considers that the UK model is not suitable for Hong Kong. It is difficult to set out a blanket statutory maximum fee for compliance with DAR. Setting the fee too low will attract abuses by the data subjects and thereby causing unacceptable financial burden on the data users in complying the request. To set the fee too high will dissuade individuals from exercising their statutory right. Furthermore, the introduction of "disproportionate effort" in the UK model to Hong Kong will create new problem in applying the condition of "disproportionate effort".

15. Having considered the above, the Commissioner recommends the introduction of the following into the Ordinance:-

    (a) a non-refundable processing fee of HK$50.00 payable upon lodgment of a DAR; and

    (b) a fees schedule setting out the maximum level of fees for additional chargeable items such as copying charges, postage, etc to be imposed by a data user on the requestor in complying a DAR.

16. The processing fee aims to cover one-hour labour cost of a junior clerical staff for handling a data access request. It will be non-refundable even when it turns out the data user does not hold any of the personal data requested. As for the fee to be imposed for complying with a DAR, any fees charged in accordance with the fees schedule will be deemed non-excessive.

17. It is intended that the proposed charging scheme will not override or affect any existing provision in any ordinance or regulation which prescribes specific fees for supplying copy of any document that contains personal data. These fees should not be regarded as excessive since they have undergone due legislative process and there are public consensus and recognition on the level of fees charged.

18. The chargeable items listed in the fees schedule is not meant to be

[11] Paragraph 85, Complaint Determination No.1 of 2004
http://www.privacy.gov.au/materials/types/determinations/view/6024#is2

exhaustive. Any fees imposed otherwise in accordance with the schedule will have to meet the existing requirement of not being excessive.

19. It is also proposed that the Commissioner shall be empowered, in consultation with Secretary for Constitutional and Mainland Affairs, to amend the fees schedule from time to time by notice in the Gazette having due regard to the consumer price index and prevailing market price of particular item.

Suggested Amendment

(A) That section 18(1) be amended by inserting "on payment of the processing fee prescribed in Schedule 7" after "may" so that the amended section will read:-

> "An individual, or a relevant person on behalf of an individual, may on payment of the processing fee prescribed in Schedule 7 make a request… …"

(B) That section 28(3) be amended by providing immediately after the existing sentence the following:-

"Any fee imposed in accordance with Schedule 7 or any provision of any Ordinance or regulation shall be deemed non-excessive."

(C) That section 71 be amended by providing that the Commissioner may, in consultation with the Secretary for Constitutional and Mainland Affairs, amend Schedule 7 from time to time by notice in the Gazette.

(D) That a new Schedule 7 be inserted in the Ordinance as follows:-

" Schedule 7

[ss.18(1), 28(2)&(3)]

Fees for compliance with a data access request

1. The processing fee for compliance with a data access request is $50[12].

[12] Hourly rate for a general office clerk of monthly salary of HK$10,025.00 ($10,025÷ 26 days ÷ 8 hours = HK$48.2) cf. Average Monthly Salaries of selected Occupations published by Census and

2. The fee for supplying a copy of the personal data requested in a data access request:-

Chargeable item	Maximum amount
Black & White Photocopying or printout	HK$1[13] per A4 or A3 copy or similar size
Colour Photocopying or printout	HK$3.5[14] per A4 or A3 copy or similar size
Postage	Not more than the charge for registered delivery of Non-Bulk Letter Mail Postage provided by Hongkong Post
Courier	Not more than the standard service of Local Courierpost provided by Hongkong Post
Colour Photo printout	HK$1.2[15] per 3R size photograph
Production of duplicate CD-R optical disc for audio recordings or visual images	HK$2.2[16] per disc
Production of duplicate DVD±R optical disc for audio recordings or visual	HK$3.2[17] per disc

---

Statistics Department http://www.censtatd.gov.hk/hong_kong_statistics/statistical_tables/index.jsp?charsetID=1&subjectID=2&tableID=028

13 Photocopying charge levied by Government departments

14 Currently charged by the Transport Department http://www.td.gov.hk/access_to_information/code_on_access_to_information/index.htm

15 Source: Price Lists from Kodakexpress.com.hk, Fotomaxonline http://www.fotomaxonline.com/images/main/tc/promo_l_23.jpg, Colour Six Laboratories Ltd http://www.colorsix.com/pricelist1.asp and Sunrise Professional Photofinishing http://www.sunrisephotohk.com/pricelist.html HK$1.2 is the round up median of all the raw data obtained from the price lists

16 Average of the raw data of the Quotations (as at 24/4/2009) obtained from the internet (i.e. ($1.96+$2.5) ÷ 2 = ($2.23~$2.2) http://www.ink-hk.com/hk-cn/product_view_ts.asp?id=1409, http://www.shop248.com/stationery/stationery.php?sub_class=2502

17 see Quotations (as at 24/4/2009) obtained from the internet (($2.6+$3.8) ÷ 2 = $3.2) http://www.shop248.com/stationery/stationery.php?sub_class=2502, http://www.ink-hk.com/hk-cn/product_view_ts.asp?id=1410

images	
Production of duplicate of radiological imaging records (e.g. X-ray film, MRI, CT Scan, PET Scan, Ultrasound)	HK$290[18] per copy
Transcription of any voice recording	HK$132[19] per page

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reason :

The introduction of a fee schedule involves a new charging mechanism which affects the existing operation. The public should be consulted and views be obtained, particularly in respect of the proposed chargeable items and the respective maximum level of fee to be charged.

[18] Currently charged by Hospital Authority for similar service offered http://www3.ha.org.hk/pwh/content/report/PAPOnote.html

[19] Currently charged by Judiciary for similar service offered http://www.judiciary.gov.hk/en/other_info/access_info/pdf/access_to_info.pdf

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 27

To give due recognition of the APEC Privacy Principles and the Cross Border Privacy Rules in the context of cross-border data flow in electronic commerce transactions.

Reasons for the Proposal

1. In November 2004, the APEC Ministers endorsed the APEC Privacy Framework. The Framework, comprises of nine APEC Privacy Principles ("the APEC Principles"), gives the baseline for member economies to follow for the purpose of facilitating the free flow of personal information across the APEC region in the context of e-commerce.

2. The APEC Principles are by and large consistent with the six data privacy principles under the Ordinance, although there exist certain discrepancies in view of the different cultural, economic and political backgrounds. In short, the six data protection principles represent a standard that is at par, if not higher than the APEC Principles.

3. In striving for effective implementation of the APEC Privacy Framework, the Data Privacy Subgroup under the Electronic Commerce Steering Group (ECSG) is now working actively to develop a cross border privacy rules (CBPRs) system under which an organization data user may commit to apply its CBPRs to activities involving transfers of personal data across borders. It is anticipated that the CBPRs system will form the accepted standard within the APEC regions in view of globalization featuring the borderless flow of personal information.

4. It is therefore timely to review whether amendment to the Ordinance is necessary in order to give due recognition to the APEC Principles and the CBPRs.

5. In addition, the APEC Privacy Framework encourages cross border co-operation amongst the participating economies on enforcement of privacy rights. Sometimes, the investigative works of the PCPD are

daunted owing to the absence of jurisdiction to deal with a specific complaint, in particular where the act was done outside Hong Kong or where the party complained against falls beyond the regulatory remit of the Ordinance. The Commissioner therefore finds it useful to refer the matter to the appropriate overseas regulatory body so that follow up action can be taken. Such act of disclosure on the part of the Commissioner is consistent with the function under section 8(g) of the Ordinance, namely, to liaise and co-operate with any person in any place outside Hong Kong performing functions similar to the Commissioner's functions under the Ordinance.

6. In order that the disclosure can be made without fear of any breach of the secrecy provisions under section 46 of the Ordinance, an exception should be provided to facilitate the transfer of information overseas as part of the whistle-blowing exercise.

Suggested Amendments

(A) That a new section 33A be added as follows:

"33A. Notwithstanding any provision to the contrary under this Ordinance, a data user may transfer personal data outside Hong Kong for the purpose of carrying out electronic commerce transactions if:-

(a) the place to which the data are to be transferred has subscribed to the APEC Privacy Framework endorsed by the APEC member economies; or

(b) the transferee of the data has been specified by [the Commissioner/an accreditation authority] as being compliant with Cross-Border Privacy Rules endorsed by the APEC member economies."

(B) That section 46 be amended by adding the following immediately after subsection (c):-

"(d) disclosing to any corresponding person or body information which appears to the Commissioner to be likely to assist such person or body to discharge its functions.

In this section, "corresponding person or body" means any person

who or body which, in the opinion of the Commissioner, has under the law of a place outside Hong Kong, functions corresponding to any of the functions of the Commissioner."

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended in view of the great impact on personal data privacy in relation to cross border flow of personal data.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 28

To exclude from the definition of "direct marketing" the offering of social services and facilities by social workers to individuals in need of such services or facilities.

Reasons for the Proposal

1. The term "direct marketing" is defined under section 34(2) of the Ordinance to mean :

   "(a) the offering of goods, facilities or services;

   (b) the advertising of the availability of goods, facilities or services; or

   (c) the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes,

   by means of-

   (i) information or goods sent to any person by mail, facsimile transmission, electronic mail, or other similar means of communication, where the information or goods are addressed to a specific person or specific persons by name; or

   (ii) telephone calls made to specific persons.

2. A liberal interpretation of the ordinary word of "services" is capable of a wide application. For instance, when a social welfare organization learns from a source that an individual is in need of its service, the offering of assistance by a social worker by letter or telephone could amount to "direct marketing" under section 34(2) for which an "opt-out" notice shall be given to the data subject in compliance with section 34(1)(i).

3. This gives rise to the result that if the individual exercises the "opt-out" right, the social worker is prohibited from using the personal data to make direct contact with him or her. This would cause serious impediment to the work of the social workers, who in the proper interest of the client and of the society at large, should continue to "knock the door" of the client, sometimes even against his or her wish. The persons who offer social services are generally those who are offering services under (a) the Social Workers Registration Ordinance, Cap 505; and (b) the social security

schemes administered by the Director of Social Welfare.

4. It would be against the legislative intent of the Ordinance for "direct marketing" activities under section 34 to be construed broadly to cover and apply to the provision of essential social welfare services for the benefits of the intended recipients. It is therefore appropriate that the definition of "direct marketing" be revised accordingly.

Suggested Amendments

That section 34 is amended by inserting an exclusion under subsection (3):–

"(3) For the purpose of subsection 2(a) and (b), the offering of goods, facilities or services and the advertising the availability of goods, facilities or services shall not include those offered and advertised by—

(a) a registered social worker in the discharge of the duties of a social work post within the meaning of the Social Workers Registration Ordinance, Cap 505; and
(b) a public officer designated by the Director of Social Welfare to render any services under the welfare system;
(c) a staff designated by the head of a SWD-subvented non-governmental organization to render any services under the welfare system.

(Remarks: Paragraphs (b) and (c) not yet finalized pending reply from Social Welfare Department)

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Not recommended for the following reason :

The proposed amendment is in alignment with public interest and hence will likely gain public support.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 29

To increase the penalty level of contravention of the misuse of personal data in carrying out direct marketing activities.

Reasons for the Proposal

1. Section 34 of the Ordinance regulates the use of personal data in carrying out direct marketing activities by data users. Pursuant to section 34(1)(ii) of the Ordinance, a data user shall not use any personal data for the purpose of carrying out direct marketing activities if the individual who is the subject of the data has requested the data user to cease to so use his personal data.

2. A data user who, without reasonable excuse, contravenes section 34(1)(ii) commits an offence under section 64(10) and is liable on conviction to a fine at level 3, i.e. a maximum penalty of $10,000.

3. Over the years, the PCPD has referred cases of suspected breach of section 34 to the police, resulting in a number of successful prosecution cases. In a case brought before the court in January 2007 concerning the making of direct marketing calls by a telecommunications company, the Magistrate remarked that the direct marketing calls were "disgusting and annoying". The maximum penalty of $10,000 imposed under the Ordinance can hardly act as an effective deterrent for large companies like the defendant. Having considered that the defendant had pleaded guilty, the Magistrate awarded a total fine of $14,000 for the four summonses filed against the defendant.

4. In view of the fact that direct marketing activities are prevalent in Hong Kong and are often a cause of complaint and nuisance to the data subjects, the Commissioner finds the level of penalty imposed under section 64(10) may not be sufficient to contain the problem. Comparison has been made to the penalty levels imposed under the recently passed Unsolicited Electronic Messages Ordinance (Cap. 593) ("UEMO") for which a more severe punishment[1] is imposed for dealing with unsolicited commercial

[1] Pursuant to section 58(2) of the UEMO, a person to whom an unsubscribed request is sent shall not

electronic messages which bears a close resemblance to the unwelcome direct marketing calls after a party has opted-out.

5. Given the escalated expectation of privacy protection calling for higher penalty level to be imposed, the Commissioner finds it appropriate to bring the maximum penalty of the contravention of section 34(1)(ii) up to a level comparable to that for committing similar offence under the UEMO in order to tackle the problem.

Suggested Amendment

That section 64 be amended by inserting a new provision whereby the penalty level of contravention of section 34(1)(ii) be increased. The penalty level to be advised by the Department of Justice.

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reason :

Since penalty level is a matter of public concern, it should be raised in the public consultation exercise and views from diverse interest groups be sought.

---

use any information obtained thereby other than for the purpose of complying with the request. According to section 58(3) of the UEMO, a person who contravenes section 58(2) commits an offence and is liable on summary conviction to a fine at level 6. By virtue of section 58(4) of UEMO, a person who knowingly contravenes section 58(2) commits an offence and is liable on conviction on indictment to a fine of $1,000,000 and to imprisonment for 5 years http://www.legislation.gov.hk/blis_pdf.nsf/6799165D2FEE3FA94825755E0033E532/BE5AA57E2A0358C7482575EF00201941/$FILE/CAP_593_e_b5.pdf.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 30

To allow the Commissioner and his prescribed officers to disclose information if it is reasonably necessary for the proper performance of his functions and the exercise of his powers without breaching the duty of secrecy under section 46(2).

Reasons for the Proposal

1. Section 46(1) imposes a duty upon the Commissioner and his prescribed officers to maintain secrecy in respect of all matters that come to his actual knowledge in the performance of his functions and the exercise of his powers. Section 46(2) provides the excepted circumstances where (i) disclosure is made in the course of proceedings for an offence under the Ordinance before any court or magistrate; (ii) the reporting of evidence of crime to such authority as the Commissioner or his prescribed officer considers appropriate; and (iii) disclosing to a person any matter which in the Commissioner's opinion may be ground for complaint by that person. Breach of the duty of secrecy is an offence under section 64(6) which attracts a penalty level of fine at level 3 and imprisonment for 6 months.

2. In the ordinary exercise of the Commissioner's functions and powers, the disclosure of such matters that come to his knowledge are sometimes necessary. For instance, disclosure may be relevant for the purpose of publishing the Annual Report, for compiling investigation report, for issuance of press release or statement, for discussing with members of the Personal Data (Privacy) Advisory Committee appointed under the Ordinance or for disclosure to a third party for the purpose of obtaining information to assist an investigation. Moreover, in handling appeals to the Administrative Appeals Board ("AAB"), information and documents possessed by the Commissioner that relate to the appeal have to be disclosed to the Board and other parties to the appeal. The past decisions given by AAB may also be quoted and referred to in handling investigations and attending AAB or other judicial proceedings. Although decisions made by the AAB are available to the public upon request, the further use of the same by the Commissioner for purposes aforesaid may technically amount to a breach of secrecy as it does not fall within any of

the excepted circumstances under section 46(2).

3. All these may arguably constitute breaches of the secrecy requirements given the restrictive construction of section 46(1) and (2) which is seen to be hindering the proper performance of the functions and the exercise of the powers of the Commissioner.

4. Reference is made to section 59 of the UK Data Protection Act 1998 which allows for disclosure of personal information if it is necessary to do so in the public interest. Exceptions to the duty of secrecy are also found in some local legislations, such as section 378 of the Securities and Futures Ordinance and section 74 of the Sex Discrimination Ordinance which permit disclosure in a number of situations associated with the proper discharge of the functions and the exercise of powers of these statutory bodies.

5. In order to enable the Commissioner to properly discharge his duties without fear for breach of section 46, the Commissioner finds it necessary to amend the scope of application of the duty of secrecy.

Suggested Amendment

That section 46(2) be amended by adding sub-paragraph (d) as a new exception to secrecy requirement:-

"(d) disclosing to any party any information to the extent that such disclosure is reasonably necessary for the proper performance of the functions and the exercise of the powers of the Commissioner or his prescribed officer under this Ordinance."

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Not recommended for the following reason :

The proposed amendment only seeks to clarify the scope of the duty of secrecy

to enable the more efficient discharge of the Commissioner’s functions and powers.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 31

To change the notice period prescribed under section 46(4)(b) from 28 days to 14 days for the data user to respond to the report proposed to be published by the Commissioner under section 48.

Reasons for the Proposal

1. The Commissioner may, after completion of an inspection or investigation, publish a report under section 48 of the Ordinance setting out the result of the investigation or recommendations or other comments arising from such inspection or investigation.

2. Sub-paragraph (b) of section 46(4) obliges the Commissioner, before publishing the report, to give the relevant data user no less than 28 days to advise on whether there is any matter contained in the report that is exempt from data protection principle 6 the disclosure in relation to which the data user objects.

3. The Commissioner finds the 28 days notice requirement to be an undue constraint. Generally speaking, the Commissioner will choose to publish a report when he considers the case involving an issue of significant social or public interest, sometimes on matter which has already been widely reported by the media. The effectiveness of sending out the message through the report will be hampered or diminished if it is not being reported timely.

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

Suggested Amendment

That subsection 4(b) of section 46 be amended by substituting “14 days” for

“28 days.”

The Commissioner’s Disposition

Supported.

Public Consultation : Recommended or Not

Not recommended for the following reason :

The proposed amendment does not have any significant privacy impact that warrants public consultation.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 32

To broaden the scope of the exemption under section 59 of the Ordinance to cover identity and location data of the data subjects.

Reasons for the Proposal

1. Section 59 exempts personal data relating to physical or mental health of the data subject from DPP3 and DPP6 when application of these provisions would be likely to cause serious harm to the physical or mental health of the data subject or any other individual. Other personal data, such as location data of the data subject are not exempted under section 59.

2. Section 59 is found to be overtly restrictive. In some situations, when the life and limb of the data subject or other individual is at stake, the provision of the location data is of equal importance to facilitate immediate access and rescue actions to be taken by the relevant authorities to prevent serious physical or mental harm to be suffered. For example, the provision by the telephone company to the police of the location data about the "999" emergency caller can speed up rescue actions to be promptly taken. In addition, the provision by the police to the Social Welfare Department of the identity and location of an individual suspected to have a social or mental problem needing appropriate attention and help is also important for the benefits of the individual in question.

3. In emergency crisis such as the 2004 East Asian tsunami catastrophe, an exemption of this nature would enable the Immigration Department to supply the location data of the missing Hong Kong people to the rescue teams and/or their relatives.

Suggested Amendment

That section 59 of the Ordinance be amended to broaden its scope of application to cover personal data relating to the location of the data subject.

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reason :

The proposal has impact on personal data privacy protection since disclosure of the location data may sometimes be viewed as objectionable from the perspective of some data subjects. The question is whether the public interest outweighs the intrusion into the personal data privacy and whether the extent of disclosure (i.e. location data only) is proportionate to the benefits to be achieved (i.e. to prevent serious bodily and mental harm). The proposal should therefore be put forward for public consultation.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 33

To create a new exemption in the form of a public interest determination to cover situations where disclosure of personal data is in the public interest despite that prescribed consent cannot be obtained from the data subject.

Reasons for the Proposal

1. Many of the exemptions under Part VIII of the Ordinance are motivated on the corresponding need to protect public interest so that a fair balance is to be struck between competing interests. However, there is no single exemption provision in the Ordinance that makes protection of public interest itself a justification for infringing the personal data privacy right of an individual. The reason is obvious. Given the fluid concept of what constitutes "public interest", it should not be a matter falling entirely upon the judgment of the data user to invoke and rely upon a general exemption provision.

2. Overseas privacy legislations are examined to find out the jurisprudential approach.

3. In UK, public interest is expressly provided in the Data Protection Act 1998 as a factor for considering whether personal data are fairly handled. For instance, Schedule 4 of the Act provides that the eighth principle (adequate level of protection) does not apply if "the transfer [of personal data] is necessary for reasons of substantial public interest". "Public interest" is also recognized as a defence to criminal offences in unlawfully obtaining of personal information[1] and unlawful requesting of employment related records[2].

4. In New Zealand, the Privacy Commissioner may grant authorization to collection, use or disclosure of personal information that was otherwise a contravention of the information privacy principle, if public interest

---

1 Section 55(2)(d) of the UK Data Protection Act 1998 http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_7#pt6-pb2-l1g55

2 Section 56(3)(b) of the UK Data Protection Act 1998 http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_7#pt6-pb3-l1g56

substantially outweighs the interference with the privacy that could result[3].

5. In Australia, the Privacy Commissioner is also empowered to make determination[4] to exempt an otherwise infringing act, after balancing the interest in doing the act and the adherence to the information privacy principle, or national privacy principle, as the case may be. The Australian Privacy Commissioner is also empowered to issue a Temporary Public Interest Determination to cater for emergency or urgent situation.

6. To confer on the Commissioner the power to give public interest determinations is desirable as it is a flexible catch-all approach to cover different situations that justify deviation from the data protection principles. The Australian example of "public interest determination" which operates on an *ad hoc* basis upon application made by the concerned party is a good model that lends useful reference.

7. Instead of creating a general public interest exemption, the Commissioner can be vested with the power to determine each application by taking into account all the circumstances of the case, including the purpose of collection or use of the personal data and the degree of intrusion into personal data privacy, etc. Approval by the Commissioner means that the act or practice in question will not be viewed as contravention of the Ordinance, and conditions can be imposed upon the data user, such as the duration of the approval, the retention and erasure of the data and the class of permitted transferee(s), etc. By confining approval on the merits of each case, it creates minimal impact upon personal data privacy.

8. The added power might result in application being made for publication of the list of sexual offenders, child abusers and misbehaved travel agents and the Commissioner will consider each application to determine whether approval should or should not be granted.

9. In order to build in regulatory flexibility when public interest outweighs the degree of intrusion into personal data privacy, it is proposed that the Commissioner be vested with the power to make public interest determination, with conditions, if any, imposed on a case-by-case basis upon application by the relevant data user.

---

[3] Section 54 of the New Zealand Privacy Act 1993
http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM297419.html

[4] Part VI of the Australian Federal Privacy Act 1988
http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/framelodgmentattachments/1B0AD21B8A87AD58CA2576080018DAEF

Suggested Amendments

(A) That new sections be inserted in Part VIII as follows:-

"[1] Where the Commissioner is satisfied that:-

(a) an act or practice of a data user contravenes, or, may contravene, any requirement under this Ordinance; and

(b) the public interest in the data user doing the act, or engaging in the practice outweighs to a substantial degree the public interest in adhering to that requirement,

the Commissioner may, upon written application of the data user, make a written determination to that effect and, if the Commissioner does so, the personal data relating to such act or practice shall be exempt from the requirement if the act is done or the practice is engaged in (in accordance with the conditions imposed under section [5], if any) while the determination is in force.

[2] (1) The Commissioner shall prepare a draft of the proposed determination in relation to the application.

(2) The Commissioner must send to the applicant for the determination and each other person (if any) who is interested to the application a written invitation to notify the Commissioner within the period specified therein whether to hold a conference about the draft determination.

[3] (1) If the data user duly notifies the Commissioner of the wish to hold the conference about the draft determination, the Commissioner shall hold such a conference.

(2) The Commissioner shall fix a day, time and place for the holding of the conference.

(3) The Commissioner shall give notice of the day, time and place of the conference to the applicant and to each person to whom an invitation was sent.

[4] (1) At the conference, the applicant is entitled to be represented by a person who is, or persons each of whom is, an officer or employee of the applicant.

(2) At the conference, a person to whom an invitation was sent, or any other person who is interested in the application and whose presence at the conference is considered by the Commissioner to be appropriate, is entitled to attend and participate personally or, in the case of a body corporate, to be represented by a person who is a director, officer or employee of the

body corporate.

[5] The Commissioner shall, after complying with sections [2], [3] and [4] in relation to the application, make:-

(a) such determination under section [1] (with or without conditions imposed) as he considers appropriate; or

(b) a written determination dismissing the application.

[6] (1) The Commissioner shall, in making determination, take account of all matters raised at the conference and all submissions made about the application.

(2) The Commissioner shall include in a determination a statement of the reasons for the determination.

(*Note: Consider whether the determination should fall within the jurisdiction of Administrative Appeals Board*)

[7] (1) This section applies if the Commissioner is satisfied that:-

(a) the act or practice of a data user that is the subject of an application under section [1] for a determination contravenes, or may contravene any requirement under this Ordinance;

(b) the public interest in the data user doing the act, or engaging in the practice outweighs to a substantial degree the public interest in adhering to that requirement; and

(c) the application raises issues that require an urgent decision.

(2) The Commissioner may make a written temporary public interest determination to that effect and, if the Commissioner does so, the personal data relating to such act or practice shall be exempt from the requirement if the act is done or the practice is engaged in (in accordance with the conditions imposed under subsection (3)(b), if any) while the determination is in force.

(3) The Commissioner must:-

(a) specify in the determination a period of up to 12 months during which the determination is in force (subject to section [8](2)(a));

(b) specify in the determination the conditions to be imposed on the act or practice, if the Commissioner thinks fit to do so; and

(c) include in the determination a statement of the reasons for the determination.

[8] (1) The fact that the Commissioner has made a temporary public interest determination about an act or practice does not prevent the Commissioner from dealing with an application for public interest determination in relation to that act or practice.

(2) A temporary public interest determination about an act or practice ceases to be in effect when:-

(a) a public interest determination about the act or practice comes into effect; or

(b) a determination is made under section [5] to dismiss the application."

(B) That a new section 64(11) be included as follows:-

"(11) A data user who contravenes any conditions imposed pursuant to section [5](a) or [7](3)(b) commits an offence and is liable on conviction to [an appropriate penalty level to be advised by the Department of Justice].

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reason :

This is a proposal that will bring about significant privacy impact and public concerns. Therefore, views from different interest groups and from society at large should be sought in the consultation exercise.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 34

To create a new exemption in the form of an emergency declaration scheme for collection and use of personal data for permitted purposes under a state of emergency or disastrous situation.

Reasons for the Proposal

1. When crisis struck Hong Kong involving mass casualties or catastrophes where victims or missing persons require immediate assistance and rescue, the Ordinance should provide a flexible mechanism for the Privacy Commissioner to take timely decision to enable exchange of personal data by the data users in order to render the necessary assistance without fear of contravention of the Ordinance.

2. Reference was made to Part VIA of the Privacy Act of Australia which came into force in December 2006. It provides for a mechanism which allows agencies and organizations to collect, use or disclose personal information of individuals involved in an emergency or disaster with less restrictions. According to the provisions, the Prime Minister or the Attorney General can make a declaration of emergency occurred in or outside Australia and for so long as the declaration remains in force, the personal information relating to an individual can be collected, used or disclosed for the prescribed permitted purposes in relation to the emergency or disaster. As a measure of privacy safeguard, criminal sanction is imposed against unauthorized secondary disclosure of personal information.

3. In contrast to the Public Interest Determination proposed to be conferred upon the Commissioner which applies only to the act or practice referred to in the application and affects specific data subject(s) mentioned in the application, an emergency declaration gives general exemption to all acts or practice for handling personal data insofar as it is covered by the terms of the emergency declaration. The Commissioner, as data privacy regulator, is in the best position to judge and decide whether the public interest in protecting the well being of the data subjects in question is so overwhelming that it justifies the extent of intrusion into their personal

data privacy by making or issuing any emergency declaration.

4. In order that this new proposal would not increase the risk of unauthorized or improper handling of the personal data by the data users, the emergency declaration shall be specific enough to spell out the permitted purposes of use, the duration and restrictions imposed and such other terms and conditions as the Privacy Commissioner thinks fit.

5. It is believed that this new power will be useful to be invoked when disasters strike, such as the East Asian tsunami happened in 2004.

Suggested Amendments

(A) That new sections be added in Part VIII to the Ordinance as follows:-

"**[1] Emergency Declaration**

Where the Commissioner is satisfied that:-

(1) an emergency or disaster has occurred (whether within or outside Hong Kong); and

(2) the emergency or disaster is of such a kind that it is appropriate (whether because of the nature or extent of the emergency or disaster, the direct or indirect effect of the emergency or disaster, or for any other reason) in the circumstances to make a declaration under this section; and

(3) the emergency or disaster has affected one or more persons,

the Commissioner may make a declaration under this section and in the form prescribed in section [2].

[2] Form of declarations

(1) An emergency declaration must be in writing and signed by the Commissioner.

(2) An emergency declaration must be published in the Gazette as soon as practicable after the declaration was made.

[3] When declarations take effect

An emergency declaration takes effect from the time at which the declaration is signed.

[4] When declarations cease to have effect

An emergency declaration ceases to have effect at the earliest of:-

(a) if a time at which the declaration will cease to have effect is

specified in the declaration – at that time; or

(b) the time at which the declaration is revoked; or

(c) the end of 12 months starting when the declaration is made.

[5] Authorization of handling of personal data

Personal data relating to a data subject who is reasonably believed to be involved in an emergency or disaster in respect of which an emergency declaration is in force are exempt from the provisions of data protection principle 1 and data protection principle 3 if the data are used or collected for a permitted purpose in relation to an emergency or disaster as defined in section [6].

[6] Meaning of permitted purpose

(1) A permitted purpose in relation to an emergency or disaster is a purpose that directly relates to an emergency or disaster in respect of which an emergency declaration is in force.

(2) Without limiting subsection (1), any of the following is a permitted purpose in relation to an emergency or disaster:-

(a) identifying individuals who are or may reasonably be suspected to be involved in the emergency or disaster;

(b) assisting individuals involved in the emergency or disaster to obtain services such as repatriation services, medical or other treatment, health services and financial or other humanitarian assistance;

(c) assisting with law enforcement in relation to the emergency or disaster;

(d) coordinating or management of the emergency or disaster;

(e) informing the immediate family members, [*de facto spouse, insurance company, employers and employees*] of the data subject appropriately of matters that are relevant to the involvement of those data subjects in the emergency or disaster or the response to the emergency or disaster in relation to those data subjects.

(3) In this section—

"immediate family member" (直系家庭成員), in relation to a person, means a person who is related to the person by blood, marriage, adoption or affinity.[1]

---

[1] The scope of the "responsible persons" in the Australian Privacy Act (clause 2.5 of Schedule) http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/framelodgmentattachments/1B0AD21B8A87AD58CA2576080018DAEF is much wider and difficult to verify, e.g. "*person who has intimate personal relationship*". The above definition of "immediate family member" taken from Family Status Discrimination Ordinance http://www.eoc.org.hk/EOC/GraphicsFolder/showfsdo.aspx?id=7937 is therefore adopted here for discussion purpose. However, it may be worth considering if "affinity" should be included.

(B) That a new section 64(12) be included as follows:-

"A person knowing that personal data were collected because of the operation of emergency declaration by the Commissioner, makes use of the personal data for any purpose other than the permitted purposes listed in section [6] commits an offence and is liable on conviction to [an appropriate penalty level to be advised by the Department of Justice].

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reason :

This proposal has significant personal data privacy impact. Therefore, views and responses from members of the public as to the scope of application of the exemption and the measures to prevent abuse should be sought.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 35

To add a new exemption for use of personal data where the use (i) is required by law or ordered by court; or (ii) relates to any legal proceedings in Hong Kong, or is otherwise related to establishing, exercising or defending legal rights.

Reasons for the Proposal

1. DPP3 limits the use of personal data for a purpose which is the same as or directly related to the original purpose of collection unless the prescribed consent from the data subject is obtained.

2. Sometimes, a data user is required by law, for instance, under a statutory provision to disclose information which may contain personal data. The Commissioner in general takes the view that where disclosure of personal data is authorized or required by law or in compliance with a court order, the disclosure falls within a consistent purpose allowed under DPP3. This view, however, was not accepted by the Administrative Appeals Board in a recent appeal[1] whereby the Board ruled that *"disclosure of personal information to public prosecution authorities could not be considered to be a 'use' of the information intended by the parties when the information was collected"*[2].

3. Hence, unless prescribed consent of the data subject is obtained or the exemption from application of DPP3 can be properly invoked under the Ordinance, a data user may run the risk of contravening DPP3 by disclosing personal data in compliance with a legal requirement or a court order.

4. The Commissioner, however, finds it reasonable and proper that insofar as the use of personal data for the purpose of legal proceedings is concerned, it is justified as an exemption from use in recognition of the right and freedom of individuals to protect or defend his own personal or proprietary rights.

---

1 AAB Appeal No. 16/2007

2 At paragraph 96 of the decision.

5. A jurisdictional study on overseas privacy legislations has been conducted. In UK, section 35 of the Data Protection Act 1998 provides for exemption of disclosure of personal data if it is required by any enactment, by any rule of law or by order of the court. In Canada, Principle 5 of the Personal Information Protection and Electronic Document Act 2000 permit disclosure of personal information with the consent of the individual or as required by law, for example, in compliance with a subpoena or warrant issued or an order made by the court or to comply with rules of court in relation to production of records.

6. In Australia, the use of personal data for a secondary purpose is allowed under Principles 10[3] and 11[4] laid down in the Privacy Act 1988 where the use or disclosure is required or authorized by or under law.

7. The New Zealand privacy legislation also allows for disclosure of personal data where it is necessary for the conduct of proceedings before any court or tribunal[5].

8. A common feature is found in overseas privacy laws exempting the use or disclosure of personal data or information when it is required or authorized by law to do so. It is therefore in the interest of clarity for the exception to be explicitly stated in the Ordinance.

Suggested Amendment

That a new section be added to Part VIII of the Ordinance as follows:-

"**Compliance with law and legal proceedings, etc.**

Personal data are exempt from the provisions of the data protection principle 3 where:-

(a) the use is required by or under any enactment or any rule of law applicable to Hong Kong, or by the order of a magistrate, court or tribunal in Hong Kong; or

(b) the use relates to any legal proceedings in Hong Kong, or is otherwise

---

3 Paragraph 1(c) of Principle 10 under section 14 of the Australian Privacy Act 1998 http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/framelodgmentattachments/1B0AD21B8A87AD58CA2576080018DAEF

4 Paragraph 1(d) of Principle 11 under section 14 of the Australian Privacy Act 1998 http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/framelodgmentattachments/1B0AD21B8A87AD58CA2576080018DAEF

5 Principle 10(c) and Principle 11(e)(iv) of the New Zealand Privacy Act 1993 http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM297038.html

related to establishing, exercising or defending legal rights.”

The Commissioner’s Disposition

Supported.

Public Consultation : Recommended or Not

Not recommended for the following reason :

The proposed amendment is in alignment with international practice and in conformity with the common law principle of open justice.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 36

To provide for a new exemption from DPP3 for personal data available in the public domain.

Reasons for the Proposal

1. Personal data gathered or obtained from the public domain by a data user are treated no differently from other personal data under the current provisions of the Ordinance.

2. Personal data can be made known in the public domain by various means, such as by being contained in public records and obtainable through public search or inspection, e.g. court documents filed, records kept by public registries, etc. Another means is by way of publication in the media, such as a journalistic report or a public announcement.

3. Question arises as to whether a data user is still required to observe the requirements under DPP3 where the personal data are available in the public domain.

4. Overseas privacy legislations are examined as to the level of protection afforded to publicly available information. In UK, although there is no general public domain exemption, the rules restricting disclosure of personal information do not apply when a data controller is required by law to make the personal information available to public whether by publishing it, or by making it available for inspection, or otherwise[1].

5. In Canada, the Personal Information Protection and Electronic Document Act 2000 allows an organization to collect or use personal information without knowledge or consent of the individual where the information is publicly available and is specified by regulation[2].

---

1 Section 34 of Data Protection Act 1998, UK http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_5#pt4-l1g34

2 Section 7(1) and (2) of the Personal Information Protection and Electronic Documents Act 2000, Canada http://laws.justice.gc.ca/en/ShowDoc/cs/P-8.6/bo-ga:s_1::bo-ga:l_1/20090728/en?page=1&isPrinting=false#codese:7

6. In New Zealand, the Privacy Act does not provide for a public domain exemption. However, section 59 of the Act establishes the public register privacy principles. Principle 2 provides that personal information obtained from a public register shall not be re-sorted or combined with personal information obtained from any other public register, for the purpose of making available for valuable consideration personal information assembled in a form in which that personal information could not be obtained directly from the register.

7. The APEC Privacy Framework has limited application to publicly available information[3]. It is stated in the Notice Principle that it may not be appropriate for personal information controllers to provide notice regarding the collection and use of publicly available information. Also, it is expressly stated under the Choice Principle that it may not be appropriate for personal information controllers to provide individuals with mechanisms to exercise choice when collecting publicly available information.

8. The Commissioner acknowledges that there are problems of using publicly available information for secondary purposes, such as the use of property owners' records from the Land Registry to provide a search of an individual's property ownership, the use of personal data contained in public register for direct marketing activities. Added to this is the improper use of personal data available on the Internet arising from data leakage incidents. On the other hand, there may be legitimate purposes to serve in checking an individual's financial status, such as property ownership, before deciding whether to institute legal proceedings or pursue enforcement actions against him.

9. It is therefore timely to consider whether personal data available in the public domain should be exempted from the data protection principles and if so, to what extent.

---

[3] The term "publicly available information" is defined as "personal information about an individual that the individual knowingly makes or permits to be made available to the public, or is legally obtained and accessed from (a) government records that are available to the public; (b) journalistic reports; or (c) information required by law to be made available to the public". http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf

Suggested Amendment

That a new provision be added to exempt personal data from the application of DPP3 where the data are available in the public domain.

The Commissioner's Disposition

Open-minded. It is appropriate to carry out a private consultation with the interested groups to ascertain the common disposition.

Public Consultation : Recommended or Not

Subject to findings from the private consultation and if response is positive, public consultation will be conducted to solicit views from a broader spectrum of interested groups.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 37

To exempt from application DPP3 where personal data of historical, research, educational, cultural or recreational interests are transferred to the Public Records Office for processing, use and retention in the exercise of its functions and activities.

Reasons for the Proposal

1. For archival purpose, government departments and organizations will transfer records of historical, educational or recreational interests to the Public Records Office for retention. The records transferred may contain personal data, hence, protected by DPP3. Since such transfer in most cases is not within the original or related purpose of collection, and in the absence of prescribed consent from the data subjects, the act may contravene DPP3.

2. The Ordinance, as it presently stands, does recognize the importance of preserving personal data of historical values. This is provided under section 26 whereby a data user is permitted to retain personal data if it is in the public interest (including historical interest) for the data not to be erased. The recent public outcry over the destruction of the logbooks of boats and vessels containing the records of the owners shows that the public concern about the preservation of records of historical value.

3. In alignment with the legislative spirit that personal data of historical value warrant preservation, the transfer of information to the Public Records Office for keeping these data clearly serves the public interest of proper records keeping. The Commissioner finds a case made out to exempt the application of DPP3 when personal data are so transferred in order to overcome the practical difficulty of obtaining the prescribed consent of the data subjects, who might not be traceable due to lapse of time.

Suggested Amendments

That a new provision of exemption from application of DPP3 be created for

transfer of personal data of historical, research, educational, cultural or recreational interests to the Public Records Office for the following purposes:-

(i) record preservation;
(ii) public access[1], including access by government agencies, either upon request or through various means including:-
    (a) presentation in conference, seminar or workshop, etc;
    (b) presentation through electronic means;
    (c) publication; and
    (d) broadcast; and

(iii) copying, exchange or sale for non-commercial purposes.

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Not recommended as a clear case of public interest is shown for use of personal data to preserve public records for the greater good of Hong Kong

[1] "Public access" includes disclosure of personal data contained in archival records pursuant to the "30-year Access Rule", which, according to the Government Records Service Director, means that "when unclassified records held in (the Public Records Offices) have been in existence for 30 years or more, they are open for public use automatically." http://www.grs.gov.hk/ws/english/faq_access.htm#1

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 38

To exempt from the application of DPP3 the transfer or disclosure of personal data in intended merger or acquisition activities or transfer of businesses of data user, provided that the resultant organization will offer substantially similar service as the original data user.

Reasons for the Proposal

1. In a volatile economic market like Hong Kong, merger, amalgamation and transfer or sale of businesses are all but common occurrences. In order to facilitate conclusion of the deal, personal data held by the original business may have to be disclosed or transferred to the interested party for such purpose as conducting due diligence or feasibility studies. Since such use of personal data may not fall within the original or directly related purpose of collection, the transfer could be inconsistent with DPP3 in the absence of prescribed consent from the data subjects. If the data subjects' prescribed consent have to be obtained before the transfer of personal data, it will pose a hurdle to merger or acquisition activities which are very often time sensitive. There may also be genuine need to keep the transaction in secret at the due diligence stage.

2. A jurisdictional study of overseas privacy legislations shows support for such an exemption.

3. In Australia, under section 13C of the Federal Privacy Act 1988, where there is a change of partnership business, neither the disclosure (by the old partnership) nor the collection (by the new partnership) of personal information that was necessary for the new partnership is act or practice that interferes with privacy provided that at least one person in the old partnership would remain as partner in the new partnership and the new partnership carries on a business that is the same or similar to the business carried on by the old partnership.

4. In New Zealand, Information Privacy Principle 11 of the Privacy Act 1993 permits disclosure of information when the agency believes on reasonable grounds that the disclosure of the information is necessary to facilitate the

sale or other disposition of the business as a going concern.

5. In Alberta, Canada, section 22 of the Personal Information Privacy Act sets out a regime for the disclosure of personal information without the consent of the subject in the course of a transaction consisting of purchase, sale, lease, merger or amalgamation or any other type of acquisition or disposal of an organization. The relevant party is obliged to destroy or return the information if the transaction is not put through. The exemption does not apply to business transaction where the primary purpose, objective or result of the transaction is the purchase, sale, lease, transfer, disposal or disclosure of personal information.

6. In the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics, recommendations were made to fine-tune the provisions of the Personal Information Protection and Electronic Documents Act ("PIPEDA"), Canada. Particularly, recommendations are made to amend the PIPEDA along the line of the Alberta's approach with the following enhancements, namely, that (i) due diligence exercise should involve the least amount of personally identifiable information possible; (ii) all affected individuals be informed of the transfer as soon as practicable after the transfer of ownership; and (iii) the new owner should adhere to the selling organization's policies respecting privacy until all individuals have had an opportunity to choose whether they want to have a relationship with the new owner.

7. In Hong Kong, the call for a specific exemption was initiated by the Government dating back to years ago when there were frequent merger of banks and the relevant merger bills were tabled before the Legislative Council for consideration. The Commissioner considers that there are justifications for such an exemption but any proposed exemption should cover the following:-

   (i) that the resultant organization or the business transferee will provide essentially the same or similar service as the original data user when their personal data were first collected;

   (ii) that only minimal personal data that are necessary for the due diligence purpose be disclosed;

   (iii) that the transferee shall only use and process the personal data within the confines of the limited purpose; and

(iv) that the personal data so transferred shall be properly destroyed or returned to the transferor when the transaction does not proceed. A proper balance is to be struck between the protection of personal data privacy interests of the data subjects and the business interests in general.

Suggested Amendments

(A) That a new exemption be added to Part VIII of the Ordinance as follows:-

"**Mergers, acquisition and transfer of business**

(1) Personal data used for the purpose of effecting a merger, acquisition or transfer of business of the data user including the prospective transaction of such a nature are exempt from the provisions of data protection principle 3 in any case where—

(a) it is not practicable to obtain the data subjects' prescribed consent for such a use;

(b) the use of the data are necessary but not excessive for that purpose; and

(c) the resultant organization or the transferee of the data will provide substantially the same or similar service to the data subjects as the original data user who holds the data.

(2) The transferee to whom the personal data are transferred or disclosed pursuant to the purpose specified in subsection (1)—

(a) shall destroy the personal data or return the data to the party that disclosed the data when the transaction is not proceeded or is not completed; and

(b) shall not use the personal data for any purposes other than those specified in subsection (1) unless the prescribed consent of the data subject is obtained or such use of the data is otherwise permitted or exempted under this Ordinance.

(3) This section does not apply to business transaction where the primary purpose, objective or result of the transaction is the purchase, sale, lease, transfer, disposal or disclosure of personal data.

(4) For the purpose of this section, the term, "transferee" means the data user to whom the personal data are disclosed under subsection (1) and the term "resultant organization" means the data user formed as

a result of the merger, acquisition or transfer of business."

(B) That a new offence be created under section 64 for contravention of subsection (2) above with an appropriate penalty level to be advised by the Department of Justice.

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reason:

The proposed amendment affects the personal data privacy interest of the data subjects and their views and response shall be sought in the public consultation exercise.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 39

To make it an offence for repeated contraventions of the Ordinance on similar facts where the first infringement has resulted in the issuance of an enforcement notice by the Commissioner.

Reasons for the Proposal

1. Under the current provisions of the Ordinance, breach of a DPP does not constitute an offence. Although the Commissioner has power to regulate the breach by the issuing of an enforcement notice under section 50, it is only when the relevant data user has contravened the enforcement notice that criminal sanction is attached under section 64(7).

2. The leniency of the Ordinance is found ineffective to guard against repeated contraventions of the DPPs. Worse still, it is technically possible for a data user who has breached a DPP and who has been served with an enforcement notice, to comply with the enforcement notice but subsequently resumes the contravening act within a short period of time. The only enforcement action that may be taken by the Commissioner is to issue another enforcement notice.

3. The Commissioner finds criminal sanction for repeated contraventions of the DPPs can serve better deterrent effect. Hence, it is proposed that the subsequent contravention of the DPP on substantially the same matter constitutes an offence.

Suggested Amendment

That a new offence be added under section 64 to the effect that a data user who, having complied with the directions in an enforcement notice served under section 50(1)(iii) to the satisfaction of the Commissioner, subsequently does an act or engages in practice which is the same or substantially similar to the act or practice for which the Commissioner had issued the enforcement notice, commits an offence and is liable on conviction to a penalty at an appropriate level to be advised by the Department of Justice.

The Commissioner’s Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reason:

Penalty level is a matter of public concern and public consultation is warranted.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 40

To increase the level of penalty for a second or subsequent convictions of section 64(7), i.e. contravention of an enforcement notice issued by the Commissioner.

Reasons for the Proposal

1. A data user who persistently refuses to comply with an enforcement notice will not just aggravate the harm caused to the data subject concerned but also show the lack of remorse for the breach in question. It also demonstrates the blatant disregard of personal data privacy, particularly when the subsequent conviction takes place within a short interval from the first one.

2. The leniency of the penalty level imposed on non-compliance with an enforcement notice is ineffective deterrence. Typical example is the continued improper use of a debtor's personal data by a debt collection agent.

3. The culpability of repeated offenders is thus more rampant than that of the first-time offender and warrants the imposition of heavier sentence. It is obviously a factor that a judge will take into account in deciding on the sentence level within the maximum penalty laid down in the Ordinance.

4. Section 64(7) as it presently stands does not provide for a heavier penalty level for repeated offenders. The judge could not order a heavier penalty than a fine at level 5 and imprisonment for two years and for a continuing offence, to a daily penalty of $1,000.

5. The Commissioner is of the view that a higher level of penalty is not excessive when dealing with repeated offenders as more severe punishment will have greater deterring effect. Reference has also been made to the Unsolicited Electronic Messages Ordinance[1] whereby a higher

[1] Section 39(1) of the Unsolicited Electronic Messages Ordinance (Cap. 593) provides that a person who contravenes an enforcement notice served on him under section 38 commits an offence. Section 39(2) states that a person who commits an offence under section 39 is liable on a first conviction, to a fine at level 6 and on a second or subsequent conviction, to a fine of $500,000, and

penalty is imposed on a second conviction for breach of an enforcement notice.

Suggested Amendments

That section 64 of the Ordinance be amended to increase the penalty for a second or subsequent convictions of section 64(7) to an appropriate level as advised by the Department of Justice.

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reason:

Penalty level is a matter of public concern and views from public and interested groups should be obtained for mapping level of acceptance and tolerance.

---

in the case of a continuing offence, to a further daily fine of $1,000 for each day during which the offence continues.
http://www.legislation.gov.hk/blis_pdf.nsf/6799165D2FEE3FA94825755E0033E532/BE5AA57E2A0358C7482575EF00201941/$FILE/CAP_593_e_b5.pdf

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 41

To create a new offence of knowingly or recklessly obtaining or disclosing personal data without consent from the data user. Sale of the data so obtained to third parties is also make an offence.

Reasons for the Proposal

1. Since contravention of a data protection principle *per se* does not attract criminal sanction, the Ordinance as it currently stands is insufficient to give protection for personal data obtained unlawfully or unfairly from the data user and thereafter disclosed or transferred in an indiscriminate fashion.

2. The following are some of the scenarios where personal data are improperly used:

   (i) the downloading and use of personal data which have been wrongfully or accidentally uploaded onto the internet by the data user;

   (ii) the unauthorized access and collection of customers' personal data by a staff of a bank or a telecommunications company for the purpose of selling them to debt collection agents or third parties for profits;

   (iii) the use of personal data for personal gains of the collector, e.g. for selling the data to direct marketing companies or for perpetuating crime by theft of identity.

3. In view of the seriousness of the intrusion into personal data privacy and the gravity of harm that may cause to the data subjects as a result of the intentional or wilful act of the person in flagrant disregard of the personal data privacy of others, due consideration should be given to make the act in question an offence.

4. Such a legislative approach is taken by the UK. Section 55 of the UK

Data Protection Act makes it an offence for any person who knowingly or recklessly, without the consent of the data controller, obtains or discloses personal data or procure such disclosure unless justifiable grounds exist, e.g. for prevention or detection of crime, or as required by or authorized by law. Section 55(4) to (6) of the Act prohibits the selling or offering to sell the personal data so obtained by making it an offence[1].

5. The Commissioner has given due regard to the following factors in proposing the present amendment :

   (i) the need to effectively address the issue of improper handling of personal data on the internet given the magnitude and scope of impact on personal data privacy when personal data can be accessed and viewed by millions of web browsers or surfers;

   (ii) to contain and regulate the situation that personal data are being traded or dealt with as a commodity which falls short of the legitimate expectation of personal data privacy of the data subjects; and

   (iii) the overseas experience in making the commission of such an act a criminal offence in giving deterrent effect[2].

6. The proposed amendment should not affect the continued operation of Part VIII exemptions to provide valid grounds to be invoked in appropriate cases.

7. As for the level of penalty, the maximum penalty provided under section 64 of the Ordinance is found to be insufficient to address the problem. A higher penalty level comparable to those under the Unsolicited Electronic Messages Ordinance[3] involving misuse of information should be followed.

---

1 Section 55 of the Data Protection Act 1998 and Sections 77 and 78 of the Criminal Justice and Immigration Act 2008 are attached for reference.

2 The UK Information Privacy Commissioner had issued a report, "What price privacy" in 2006 to review the adequacy of the level of penalty and it was suggested that apart from fine, upon conviction on indictment, the court should be empowered to give imprisonment sentence of up to two years.
http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/what_price_privacy.pdf

3 Under section 58(3) and (4) of the Unsolicited Electronic Messages Ordinance (Cap. 593), a person who contravenes section 58(1) or (2) (offences relating to misuse of information) is liable on summary conviction to a fine at level 6, and a person who knowingly contravenes the provisions is liable on conviction on indictment to a fine of $1,000,000 and to imprisonment for 5 years.
http://www.legislation.gov.hk/blis_pdf.nsf/6799165D2FEE3FA94825755E0033E532/BE5AA57E2A0358C7482575EF00201941/$FILE/CAP_593_e_b5.pdf

Suggested Amendments

That a new section modeling on section 55 of the UK Data Protection Act be added in order to deal with the situations identified in paragraphs 1 and 2 above.

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reason:

The introduction of a new offence is an important issue that requires public scrutiny. Responses from different interest groups and members of the public should be sought from the consultation exercise.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 42

In complying with DPP1(3), it shall be sufficient for a data user to state either the name or the job title of the individual to whom a data access request may be made.

Reasons for the Proposal

1. DPP1(3)(b)(ii)(B) imposes a duty upon a data user to explicitly inform the data subject on or before collection of his personal data of the *"name and address of the individual to whom any [data access/correction] request may be made"*.

2. The requirement is overly restrictive for the following reasons :

   (i) it does not take into account the possible change in personnel to handle such request ; and

   (ii) the responsible personnel may find it objectionable for his or her name and address to be made known while the giving of his or her job title would suffice for the purpose of contact.

3. The amendment is desirable for clarifying the scope of duty of the data user to give the personal information collection statement and how the duty is discharged.

Suggested Amendments

That DPP1(3)(b)(ii)(B) in Schedule 1 of the Ordinance be amended by adding the "or job title" after the word "name". Corresponding amendment shall also be made to paragraph 6 in Schedule 3 of the Ordinance.

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Not recommended for the following reason:

The amendment is tidying up exercise only and will have no impact upon personal data privacy.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 43

A data user is taken to have complied with DPP2(2) and section 26 of the Ordinance insofar as it has taken all practicable steps to erase personal data no longer required for fulfillment of the purpose of use.

Reasons for the Proposal

1. According to section 26 of the Ordinance, a data user shall erase personal data held by it where the data are no longer required for the purpose (including any directly related purpose) for which the data were used unless such erasure is prohibited under any law or it is in public interest that the data not to be erased. The duty is also laid down in the data retention principle under DPP2(2) so that personal data shall not be kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data are or are to be used.

2. Unlike the duty under DPP1(3), DPP2(1), DPP4 and DPP5 requiring only "all (reasonably) practicable steps"[1] be taken, the duty imposed under section 26 and DPP2(2) is an absolute one. The burden imposed on data users is onerous as sometimes it is not practicable for data users to meet the requirement by going through item by item the data contained in a document to delete those that are no longer required for fulfillment of the purpose of use. Particularly, if the documents are stored on microfiche, it might be practically impossible to delete only a piece of data contained in a document.

3. It may cause injustice to a data user who has exercised reasonable care and caution in regular erasure of unnecessary personal data but yet might still contravene the requirement for technical reason. To ameliorate the situation and for the sake of consistency with the standard of care imposed in other data protection principles, it is proposed that the duty imposed upon a data user under section 26 and DPP2(2) shall not be an absolute one but only to the extent that all reasonably practicable steps have been taken.

---

[1] The word "practicable" is defined under section 2(1) of the Ordinance as meaning "reasonably practicable". http://www.pcpd.org.hk/english/ordinance/section_04.html

Suggested Amendments

That section 26 be amended by adding the words, “take all practicable steps to” after the words “shall” appearing in sub-sections (1) and (2)(a) and that DPP2(2) be amended by adding the words “All practicable steps shall be taken to ensure that” at the beginning of the sentence.

(Remarks: The word “practicable” is defined under section 2(1) of the Ordinance as meaning “reasonably practicable”.)

The Commissioner’s Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reason:

The amendment will have the effect of relaxing the obligation imposed upon data users in data retention and as such will affect the personal data privacy interests of individuals. Given the impact that it brings, public consultation is needed.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 44

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 and to require any person to give information in order to verify the information stated in the return. Clerical error in section 14(9)(c) shall be made good.

Reasons for the Proposal

1. Section 14 empowers the Commissioner to specify a class of data users, by notice in the Gazette, to submit data user returns. The data user return shall be in specified form and shall contain the prescribed information set out under Schedule 3 of the Ordinance. Such information includes name and address of the data user, the kind of personal data collected, the purposes of collection, the classes of transferees of the data, the places to which the data will be transferred outside Hong Kong and the name and address of the individual to whom data access request may be made.

2. In order to give flexibility to take into account the changing needs and aspiration of personal data privacy, it is found desirable that the Commissioner be given the power to amend, add to, vary or modify the classes and nature of information required to be submitted by a data user under Schedule 3 of the Ordinance.

3. In addition, in order to ensure that the information filed by the data user in the return is accurate and no false or misleading information is stated, the Commissioner should be given the power to request any person to give information for the purpose of verifying the information stated in the data user return as and when he sees fit.

4. There is a clerical error found in section 14(9)(c) in that the subsection mentioned therein should be subsection (4) instead of subsection (3) in relation to the Commissioner's power to prescribe form for the data user return under section 67(4)(c) of the Ordinance.

Suggested Amendments

(A) That section 14 be amended by conferring powers upon the Commissioner:-

(i) by notice in the Gazette to specify and to amend the "prescribed information" under Schedule 3 of the Ordinance; and

(ii) to require persons to supply information in order to verify the information stated in the data user return.

(B) That section 14(9)(c) of the Ordinance be amended by replacing the words "subsection (3)" with "subsection (4)".

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reason:

The suggested amendments in (A) above affect the interests of data users. It is therefore necessary to carry out public consultation to solicit views and responses from the data users and members of the public.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 45

To replace the words "computer technology" under section 8(1)(f) of the Ordinance by "information technology".

Reasons for the Proposal

1. Section 8(1)(f) confers powers upon the Commissioner to undertake research into and monitor developments in the processing of data and *computer technology* in order to take into account any likely adverse effects such developments may have on the privacy of individuals in relation to personal data.

2. The use of the word "computer technology" may be construed restrictively and it is therefore advisable that a more generic term of "information technology" be used instead to cover technological advance such as RFID, Smart ID, electronic health records, etc.

Suggested Amendments

That section 8(1)(f) be amended by replacing the words "computer technology" by "information technology".

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Not recommended because it is minor and technical amendment only.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 46

To replace the word "Commission" under section 31(1)(b) of the Ordinance by "Commissioner".

Reasons for the Proposal

1. Section 31 of the Ordinance deals with the making of data matching procedure request by a data user to the Commissioner.

2. Legislative oversight in subsection (1)(b) was found by using of the word "Commission" which in fact should mean "Commissioner".

Suggested Amendments

That section 31(1)(b) be amended by replacing the word "Commission" by "Commissioner".

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Not Recommended for the following reason:

Rectification of clerical error only.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 47

To replace the word "人" appearing in section 33(1)(b) by "資料使用者".

Reasons for the Proposal

1. The Chinese version of section 33(1)(b) is inconsistent with the English version in which the words "data user" are used.

2. In order to achieve consistency and accuracy, the Chinese version of section 33(1)(b) shall be amended accordingly.

Suggested Amendments

That the Chinese version of section 33(1)(b) be amended by replacing the word "人" by "資料使用者".

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Not Recommended for the following reason:

Clarification on inconsistency only.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 48

To relieve the obligation of the Commissioner to notify the complainant the result of an investigation and related matters where the complainant has withdrawn the complaint.

Reasons for the Proposal

1. Section 40 of the Ordinance confers powers upon the Commissioner that if he is of the opinion that it is in public interest to do so, he may carry out or continue an investigation initiated by a complaint notwithstanding that the complainant has withdrawn the complaint.

2. The section goes on to provide that "the provisions of this Ordinance shall apply to the complaint and the complainant as if the complaint had not been withdrawn". The effect is that the Commissioner is still obliged under section 47(3) to notify the complainant the result of his investigation and the related matters as stated in the provision. This creates an anomaly in keeping the complainant informed while he or she has already withdrawn the complaint.

3. The decision to carry out or continue with an investigation by the Commissioner notwithstanding the withdrawal of the complaint is analogous to the exercise of the power under section 38(b) on his volition when the Commissioner has reasonable ground to believe that there is contravention of the requirement of the Ordinance. Where the Commissioner exercises the power under section 38(b) and completed an investigation, he is only obliged to inform the relevant data user under section 47(2) of the results of the investigation and the related matters.

4. In order to rationalize the situation, it is proposed that section 40 be amended so that the investigation shall hence be treated as if it was initiated by the Commissioner under section 38(b). The amendment is desirable as the Commissioner will not have to disclose further or other information unnecessarily to the party who has withdrawn the complaint. Disclosure of such information may also be seen to be in conflict with the duty of secrecy under section 46 of the Ordinance.

Suggested Amendments

That section 40 of the Ordinance be amended by replacing the words “to the complaint and the complainant as if the complaint had not been withdrawn” by “as if the investigation was initiated by the Commissioner pursuant to section 38(b)”.

The Commissioner’s Disposition

Supported.

Public Consultation : Recommended or Not

Not Recommended for the following reason:

Technical amendment not affecting personal data privacy right.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 49

To amend section 47 to allow the Commissioner to serve enforcement notice together with the results of investigation upon the relevant data user.

Reasons for the Proposal

1. Section 47(2)(d) and 47(3)(e) requires the Commissioner to notify the relevant data user and the complainant respectively whether he "proposes to serve an enforcement notice" on the relevant data user. The word "proposes" used in the section may create the impression upon the data user that it may still contest or give representations to object the issuance of the enforcement notice. It will delay the process of issuing an enforcement notice.

2. To enable the Commissioner to serve an enforcement notice to direct the relevant data user to take remedial actions as soon as possible, it is therefore desirable that section 47 be amended to remove any doubt or uncertainty by the use of the word "proposes".

3. Similar concerns are found in section 47(3)(f) and 47(4)(a) when the Commissioner "proposes not to" issue an enforcement notice, which call for tidying up amendments on the wording used.

Suggested Amendments

That section 47(2)(d) and (3)(e) be amended by deleting the word "proposes" to be replaced by "decides". Section 47(3)(f) and (4)(a) of the Ordinance be amended by deleting the words, "does not propose to" to be replaced by "decides not to".

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Not Recommended for the following reason:

Technical amendment not affecting personal data privacy right.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 50

Item 4(a) of Schedule 5 of the Ordinance to be amended to make good an omission.

Reasons for the Proposal

An omission was found in item 4(a) of Schedule 5 of the word “of” after the words, “in respect”.

Suggested Amendments

To add the word “of” after the words “in respect” in item 4(a) of Schedule 5 to make good the omission.

The Commissioner’s Disposition

Supported.

Public Consultation : Recommended or Not

Not Recommended for the following reason:

Omission made good.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 51

To introduce a mandatory data breach notification requirement on data users.

Reasons for the Proposal

1. The series of data losses incidents involving organizational data users happened recently have aroused public concern about data security as well as the containment of damage caused to the data subjects in consequence of these incidents.

2. The Commissioner observes that agencies and organizations are storing vast amounts of personal data electronically, some of which are sensitive in nature. The leakage of such data may allow identity theft of the affected individuals. The Commissioner has also learnt through his investigative works that electronic leakage of personal data, e.g. through the Internet, is difficult to contain. By the time a complaint is made to the Commissioner, the personal data could have been downloaded and retained by countless unauthorized users on the Internet. Therefore, an early response to data leakage is crucial for protecting electronically stored personal data.

3. In the circumstances, serious consideration should be given to a containment plan data users should follow in order to mitigate or reduce the damages that may cause to the data subjects. Apart from other remedial measures, data users should be required to notify the affected individuals of the privacy breach as soon as practicable after occurrence of the breach.

4. Mandatory data breach notification requires data users to notify the Commissioner as well as affected individuals when their personal data have been leaked to unauthorized individuals or organizations. This enables the affected individuals to take steps to prevent misuse of their personal data. It is intended to be a duty additional to the requirement of DPP4 which imposes obligations on data users to take all reasonably practicable steps to safeguard the security of personal data held by them.

5. Although data breach notification is not a direct measure in preventing data

leakage, it is a way to contain further spreading of the leaked personal data, and in turn minimizes the exposure of the data subjects to possible damage. This is particularly so when a significant number of data subjects are affected by the breach and where sensitive personal data are lost or stolen. The Independent Police Complaints Council ("IPCC") data leakage incident (see the investigation report) is a good example where sensitive personal data were leaked on the Internet and the affected individuals have to be notified in order that they may take steps to prevent misuse of their personal data. In that case, the IPCC gave the notification voluntarily.

6. The Commissioner has considered the positions in other jurisdictions in relation to data breach notification. In the US, over 30 States have incorporated in their state laws a duty to notify individuals of leakage of personal information. While the UK, Canada, Australia and New Zealand do not have similar provisions under their respective privacy laws, there have been accentuated voices in those territories urging for the imposition of such a statutory duty. For instance, mandatory data breach notification is introduced in the reform of the Canada data protection law (see Advance Preview of PIPEDA 2.0), and the "Approaches to Security Breach Notification: A White Paper (9 January 2007)" was issued by the Canadian Internet Policy and Public Interest Clinic setting out the Canadian model of mandatory data breach notification. In Australia, the Australian Law Reform Committee Report issued in August 2008 (recommendation 51-1) has suggested amendment to the Australian Privacy Act to introduce mandatory data breach notification.

7. Research conducted by the Commissioner's Office shows that in making provisions for mandatory privacy breach notification, regards must be given to the following elements:-

   (1) The circumstances under which notification should be triggered;

   (2) To whom the notice of security breach be sent;

   (3) The time for sending the notice;

   (4) By what means should the notice be sent, i.e. electronically, by post or otherwise;

   (5) The contents to be covered in the notice; and

   (6) The consequences for failing to give notification.

8. Although many overseas jurisdictions have not made data breach notification a mandatory requirement, the frequent incidents of electronic data losses reported locally, particularly associated with the widespread use of portable electronic devices calls for a tighter control. A speedier legislative pace on its introduction is warranted.

9. Introduction of mandatory breach notification would require additional resources for the Commissioner to carry out incidental works, such as examining each notification, considering what measures to be adopted and what follow-up actions should be taken (including investigation, compliance checks or inspection, etc, as the need arises), and handling new complaints about failure to give such notification. Leakage of personal data on the Internet may easily bring in an influx of complaints. When systematic inadequacy is detected, it may be necessary to conduct an inspection on the personal data system in question. Following the patients' data loss incident of the Hospital Authority, in which the Commissioner exercised his power to inspect the Authority's personal data system, it is envisaged that more inspections will be carried out upon notification of data breach by the data users.

Suggested Amendments

To introduce data breach notification requirement based on the Canadian model as set out in page 24 to 30 of the "Approaches to Security Breach Notification: A White Paper."

The Commissioner's Disposition

Supported a mandatory notification requirement to cover the public sector in the first place, and the private sector to follow at a later stage.

Public Consultation : Recommended or Not

Recommended for the following reason:-

Since the proposed amendments have general impact on data users and data subjects and require allocation of additional resources, public responses should be sought.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 52

To confer power on the Commissioner to require data users to pay monetary penalties for serious contraventions of data protection principles.

Reasons for the Proposal

1. At present, a person who contravenes the data protection principles faces no sanction unless he does so in non-compliance of an enforcement notice issued by the Commissioner. Although an aggrieved individual may institute a civil claim against the data user under section 66 to seek compensation, the Commissioner is not aware of any award of damages having been made by the court since the commencement of the Ordinance more than 13 years ago. A data user who takes the risk of contravening the principles has little to fear. He will not be required to pay any monetary penalties, or even costs.

2. It is obvious that there is no effective punishment or deterrent on those who knowingly or recklessly failed to comply with the requirements of data protection principles, thereby creating a risk that substantial damage or distress will be caused to any person.

3. In UK, the Government realized the inadequacy of sanction to tackle serious breaches of the data protection law. To tackle the issue, the recently enacted Criminal Justice and Immigration Act 2008 has amended the Data Protection Act by inserting a new section 55A conferring on the Information Commissioner a new power to require data users to pay monetary penalty[1].

4. Under section 55A of the Act, the Information Commissioner may serve a data controller with a monetary penalty notice if the Information Commissioner is satisfied that:-

[1] Section 144 Criminal Justice and Immigration Act 2008 inserting section 55A Power of Commissioner to impose monetary penalty. A full version of section 144 of the Criminal Justice and Immigration Act 2008 can be found at Criminal Justice and Immigration Act 2008 (c. 4).

(a) there has been a serious contravention of data protection principles by the data controller,
(b) the contravention was of a kind likely to cause substantial damage or substantial distress, and
(c) either the contravention was deliberate OR the data controller knew or ought to have known that there was a risk that the contravention would occur and that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but failed to take reasonable steps to prevent the contravention.

5. There are also provisions in the new sections 55B, 55C, 55D and 55E setting out the procedural aspects and the enforcement of such monetary penalty. The amount of penalty determined by the Information Commissioner must not exceed the amount as prescribed by the Secretary of State. An appeal mechanism is also provided. The Information Commissioner is also required to issue guidance on how he is going to exercise the functions under the new provisions.

6. Recently, there have many data losses or leakage incidents involving sensitive personal data held by the public sector as well as the private sector. The Commissioner finds that a more direct means of regulating contravention of the data protection principles will be offered if equivalent provisions similar to the UK provisions are added to the Ordinance. The power to impose monetary penalty will have to be exercised within a clearly defined statutory framework and the level of penalty must be within the range as prescribed by the Government from time to time. The proposal will hopefully deter serious contravention of the data protection principles.

Suggested Amendment

(A) That a new provisions modeling on sections 55A, 55B, 55C, 55D and 55E of the UK Data Protection Act be added.

(B) That an appeal may be made to the Administrative Appeals Board against the monetary penalty notice by the relevant data user not later than 14 days after the notice was served.

(C) That consequential amendments be made to the Administrative Appeals Board Ordinance (Cap 442).

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reason :

The introduction of a new penalty and the penalty level are matters of public concern. It should be raised in the public consultation exercise and views from diverse interest groups be sought.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 53

To confer power on the Commissioner to award compensation to the aggrieved data subjects.

Reasons for the Proposal

1. A data subject who suffers damage by reason of a contravention of a requirement under the Ordinance by a data user in relation to his personal data is entitled to compensation from the data user for that damage under section 66 of the Ordinance.

2. At present, only the court can determine the compensation under section 66 of the Ordinance. Over the years, the Commissioner notices that the provision is rarely invoked and civil claims of this kind are uncommon. There has been no reported case found where compensation was awarded. One possible reason is due to the lengthy and costly litigation process.

3. In the past, the Commissioner has encountered criticisms from some complainants that the Commissioner lacks the power to award compensation after conclusion of an investigation. It is suggested that a quick and effective mechanism be introduced to redress the situation.

4. The Australian Privacy Act empowers the Privacy Commissioner to determine after investigation a specified amount by way of compensation to a complainant for the loss and damage suffered (including injury to feelings and humiliation suffered) by reason of the act or practice complained against[1]. The Commissioner may also determine such amount to be reimbursed to the complainant for expenses reasonably incurred in connection with the making of the complaint and the investigation[2].

5. The Commissioner proposes that the Australian model be adopted. An aggrieved individual may then have an option to decide whether to

---

1 Section 52(1)(b)(iii) and section 52(1A) of the Australian Privacy Act 1988. A full version of the section can be found at ComLaw Act Compilations - Attachment - Privacy Act 1988

2 Section 52(3) of the Australian Privacy Act 1988 ComLaw Act Compilations - Attachment - Privacy Act 1988

institute a court action which is generally timely and costly or to seek compensation through this proposed procedure which is simple and quicker. The maximum amount to be awarded by the Commissioner will be set by the Legislative Council.

Suggested Amendment

(A) That a new section modeling on section 52 of the Australian Privacy Act regarding the award of compensation be added.

(B) That an appeal may be made to the Administrative Appeals Board against the determination of compensation by the relevant data user not later than 14 days after the notice of the determination was served.

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reason :

Introduction of a new mechanism for awarding compensation is a matter of public concern. It should be raised in the public consultation exercise and views from diverse interest groups be sought.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 54

To confer power on the Commissioner to provide legal assistance to persons who intend to institute legal proceedings under section 66 of the Ordinance as he sees fit.

Reasons for the Proposal

1. At present, a data subject who suffers damage by reason of a contravention of a requirement under the Ordinance by a data user in relation to his personal data is entitled under section 66 of the Ordinance to compensation from the data user for that damage. The Ordinance, however, does not empower the Commissioner to provide assistance to aggrieved data subjects in respect of legal proceedings under section 66. These individuals will need to bear all the legal costs themselves unless they are qualified for and have successfully obtained legal aid.

2. The Law Reform Commission in its report on "Civil Liability on Invasion on Privacy" published in December 2004 recommended that the Ordinance should be amended to enable the Commissioner to provide legal assistance to persons who intend to institute proceedings under section 66 of the Ordinance[1] along the lines as offered by the Equal Opportunities Commission ("EOC") under section 85 of the Sex Discrimination Ordinance (Cap.480) and section 81 of the Disability Discrimination Ordinance (Cap.487) ("the Anti-discrimination Ordinances").

3. Under the Anti-discrimination Ordinances, the EOC is empowered to assist individuals who wish to pursue compensation through legal proceedings by :

   (a) giving advice;

   (b) arranging for the giving of advice and assistance by a solicitor or counsel;

[1] See recommendation 1 on page 43 of the LRC Report on Civil Liability on Invasion on Privacy http://www.hkreform.gov.hk/en/docs/rprivacy-e.pdf.

(c) arranging for the representation by a solicitor or counsel; and

(d) providing any form of assistance which the EOC considers appropriate.

4. The granting of legal assistance will be determined on whether the case raises a question of principle or whether it is unreasonable, 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, to expect the applicant to deal with the case unaided.

5. The Commissioner notes that although the Ordinance provides recourse to civil remedy in case of intrusion into personal data privacy, this has seldom been invoked. If the Commissioner is empowered to offer legal assistance to an aggrieved data subject who suffers damage to seek redress under the Ordinance, the aggrieved party will be in a better position to assess the chance of success of his civil claim and will not be inhibited to file a lawsuit due to cost considerations. This proposal, if pursued, could achieve greater deterrent effect against acts or practices which intrude into personal data privacy, and enhance the overall effectiveness of sanctions provided for under the Ordinance.

Suggested Amendment

That a section modeling on section 85 of the Sex Discrimination Ordinance (Cap.480) be added.

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Recommended for the following reason :

Since the provision of legal assistance will require extra resources, it should be raised in the public consultation exercise and views from diverse interest groups be sought.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 55

To specify in section 19 of the Ordinance that the proper means for a data user to notify the data requestor whether he/she holds the requested data is in writing.

Reasons for the Proposal

1. At present, a data subject may make two types of data access requests to a data user under section 18(1) as follows:-

   (a) a request to inform him whether the data user holds his personal data (section 18(1)(a) request); and
   (b) a request that if the data user holds such data, to be supplied by the data user with a copy of such data (section 18(1)(b) request).

2. A data user is required under section 19(1) to comply with a data access request within 40 days after receiving the request.

3. Pursuant to section 18(2), a data access request under both section 18(1)(a) and section 18(1)(b) shall be treated as being a single request. Moreover, in accordance with section 18(3), a section 18(1)(a) request may, in the absence of evidence to the contrary, be treated as including a section 18(1)(b) request. Accordingly, in complying with a data access request (whether under section 18(1)(a) or 18(1)(b) or both), the supply of a copy of the requested data would be sufficient to discharge the data user's obligation under section 19(1), if the data user holds the data at the time of the receipt of the request. However, if the data user does not hold the data, there is no explicit provision that the data user is required to inform the requestor in writing of this.

4. Until a recent decision in the Administrative Appeals Board in AAB No. 1/2008 in December 2008, it had been the Commissioner's view that data users who so inform the data requestors verbally should not be considered a contravention of the Ordinance.

5. The Administrative Appeals Board noted that section 18 does not provide for the manner to comply with a data access request. However, the fact

that "inform" in section 18(1)(a) is not qualified, without more, does not enable the data user to comply with the request by verbal means. In the Board's opinion, bearing in mind that a data access request is required to be made in writing and a data correction request is also required to be in writing and further section 19 requires notices to the requestor have to be in writing, it would be unreasonable, if not absurd, to suggest that a requestor needs only be verbally informed by a data user that no personal data of his are held without being inconsistent with the requirements of section 19.

6. The Commissioner does not disagree with the Board that it would be reasonable to require the data user to so inform the data requestor in writing. However, the Commissioner finds that it is difficult to enforce the law in accordance with the interpretation of the Board given that the Ordinance does not expressly require the data user to so inform the data requestor in writing. According to *Francis Bennion's* Statutory Interpretation, 3rd edition, one of the rules of statutory interpretation is the "principle against penalisation under a doubtful law". At p.637, it reads as follows:-

> *"**Section 271. Principle against penalisation under a doubtful law***
>
> *It is a principle of legal policy that a person should not be penalised except under clear law (in this Code called the principle against doubtful penalisation). The court, when considering, in relation to the facts of the instance case, which of the opposing constructions of the enactment would give effect to the legislative intention, should presume that the legislator intended to observe this principle. It should therefore strive to avoid adopting a construction which penalizes a person where the legislator's intention to do so is doubtful, or penalizes him or her in a way which was not made clear."*

7. In reliance of the above statutory interpretation and bearing in mind that a contravention of section 19 attracts criminal sanction under section 64(10), the Commissioner is of the view that a person should not be put in peril of committing a crime upon an ambiguity. The Ordinance should be amended to achieve certainty and ensure understanding by members of the public of the relevant requirement under the Ordinance.

Suggested Amendments

That 19 of the Ordinance be amended to expressly require a data user to inform the requestor in writing as to whether the data user holds the requested data.

The Commissioner's Disposition

Supported.

Public Consultation : Recommended or Not

Not recommended for the following reason:-

The proposed amendment only gives effect to the Board's decision and helps the public to know how a data access request can be complied with.

Proposals to amend the Personal Data (Privacy) Ordinance, Cap 486

Proposal No. 56

To amend Data Protection Principle 4 in Schedule 1 to make it explicit that a data user is required to take all practicable steps to prevent the loss of personal data.

Reasons for the Proposal

1. Data Protection Principle 4 ("DPP4") provides that *"all practicable steps shall be taken to ensure that personal data … held by a data user are protected* ***against unauthorized or accidental access, processing, erasure or other use****…(emphasis added)".* It is not made explicit that failure to take practical steps to prevent loss of personal data held by a data user is a contravention of the principle.

2. In a recent Administrative Appeal Board case No. 26/2007 (which decision is still pending), the data user, a hospital, took up the issue arguing against contravention of DPP4 in relation to the loss of x-ray films of its patient. The Commissioner in that case examined the system of the data user in handling X-ray films and issued an Enforcement Notice on the data user directing it to take remedial steps to prevent possible future losses. The hospital challenged the Commissioner's decision by arguing that it cannot be inferred from the ***"mere loss"*** of the X-ray films that there must be ***"unauthorized or accidental access, processing, erasure or other use"*** as stipulated under DPP4. The hospital also made reference to some statistical information in order to support the saying that it is highly improbable that the "unauthorized or accidental" acts have ever taken place. As a result, it could not be inferred from the evidence that "all practicable steps" to protect the X-ray films against the "unauthorized or accidental" acts have not been taken and will not be taken in the future.

3. According to the legislative history of the Ordinance, DPP4 was legislated in response to the OECD Security Safeguards Principle which provides as follows:[1]

[1] See para 12.18 of Chapter 12 of LRC's "Report on Reform of the Law Relating to the Protection of Personal Data (Topic 27)" http://www.hkreform.gov.hk/en/docs/rdata-e.pdf.

"Personal Data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data."

The duty of a data user is to protect personal data against such risks and that such risks exist independent of the occurrence of the underlying acts.

4. A study on the overseas privacy legislations shows that similar data security principles have made it explicit that reasonable steps must be taken by the data users to protect personal data held by them from "***loss***".

5. In Australian Privacy Act 1988, National Privacy Principle 4 in Schedule 3 provides that an organisation must take reasonable steps to protect the personal information it holds from misuse and **loss** and from unauthorized access, modification or disclosure.

6. In Canada, the Personal Information Protection and Electronic Documents Act, Principle 7 in Schedule 1 states that that personal information shall be protected by security safeguards appropriate to the sensitivity of the information. Principle 4.7.1 provides that the security safeguards shall protect personal information against ***loss*** or theft, as well as unauthorized access, disclosure, copying, use or modification.

7. In the UK, Data Protection Act 1998, Part II, Schedule I, the 7th Principle states that "having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to (a) the harm that might result from such unauthorized or unlawful processing or accidental ***loss***, destruction or damage as are mentioned in the seventh Principle, and (b) the nature of the data to be protected".

8. In New Zealand, Privacy Act 1993, Part 2 Information Privacy Principle 5 states that "an agency that holds personal information shall ensure that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against (i) ***loss***; and (ii) access, use, modification, or disclosure, except with the authority of the agency that holds the information and (iii) other misuse,……".

9. In alignment with the legislative spirit of the Ordinance and the overseas privacy legislations, the Commissioner recommends the amendment of DPP4 to make it explicit that a data user is required to take all practicable

steps to safeguard against loss of personal data.

Suggested Amendments

To insert the word *“loss”* before the word *“unauthorized or accidental access”* in DPP4 so as to read *“all practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against* ***loss,*** *unauthorized or accidental access, processing, erasure or other use having particular regard to…”.*

The Commissioner’s Disposition

Supported.

Public Consultation : Recommended or Not

No, it is only a technical amendment.

Review of Personal Data (Privacy) Ordinance, Cap 486

Issues for public consultation

Issue No. 1

That the definition of "personal data" under section 2(1) of the Ordinance be amended by deeming IP address as personal data

Reasons for the Proposal

1. The Yahoo's case gave rise to public concerns about disclosure of personal data of email subscribers by email service providers. Concerns had been raised by a Legislative Council member, Mr. Sin Chung-kai, the then Chairman of the Panel on Information Technology and Broadcasting in a meeting held in May 2006 as to whether the Government should review the Ordinance and adopt measures to prohibit the disclosure of IP addresses to third parties by email service providers without the authorization of the subscribers.

2. Overseas privacy legislations as well as international guidelines or directives are examined and it is concluded that there is no universally or internationally recognized definition on "personal data".

3. The definition of "personal data" under section 2(1) of the Ordinance is capable of a wide scope of literal interpretation given the use of such terms as "indirectly" relate to a living individual and from which it is practicable for the identity of the data subject to be directly or "indirectly" ascertained.

4. The question whether IP address alone was sufficient to constitute personal data was examined in the Yahoo's case. According to the Senior Counsel's advice obtained by the Commissioner, what is not readily obtainable by the data user does not meet the "reasonably practicable" test in the definition of "personal data". Since an IP address alone can neither reveal the exact location of the computer nor the identity of the computer user and the subscriber's information is not readily obtainable, it is not caught under the definition of "personal data". However, whether IP address together with other data can constitute "personal data" will depend on the specific facts and circumstances of the case.

5. The legal research conducted by the Legal Services Division of the Legislative Council Secretariat supported the adoption of a narrow approach on the interpretation of the term "personal data" and shared the view that IP address alone is not "personal data".

6. The Commissioner completed investigation of the Yahoo's case in March 2007 and published a report pursuant to section 48(2) of the Ordinance. The Commissioner found that there was no contravention of the requirements of the Ordinance because there was insufficient evidence to prove that the complainant's personal data were disclosed.

7. Dissatisfied with the Commissioner's decision, the complainant lodged an appeal with the Administrative Appeals Board.[1] In dismissing the appeal, the AAB found that the IP log-in information provided by Yahoo, even coupled with other information disclosed, did not constitute "personal data" as defined under the Ordinance. In relation to IP address, the AAB specifically stated in paragraph 67 of the decision as follows:-

> *"It is therefore the case that the Email address, or the IP address, did not ex facie reveal the identity of the Appellant. The information provided by Beijing Yahoo! only disclosed that the email was sent from a computer located at the address of a business entity, and the date and time of the transaction. Short of CCTV evidence, it would not be reasonably practicable from such information to ascertain that it was actually the Appellant who used the computer identified by the IP address to send out the relevant email at the material time. It could have been anyone, as long as he had access to that computer (or had the necessary password if one was required at all)."*

8. Since IP address is an address that primarily attaches to a computer, as opposed to a living individual, if IP address is deemed "personal data", it will give rise to other issues of concern. For instance, should the definition of "personal data" be also extended to cover car registration number, Autotoll tag number, Octopus card number (for non-personalized card), etc. for the sake of consistency?

---

[1] AAB Appeal No. 16/2007

The Commissioner's Disposition

Open-minded.

Public Consultation : Recommended or Not

Recommended for the following reason:

The same privacy concerns may also extend to apply to other information, such as email address, mobile phone number, car registration number, etc. The Commissioner opines that strong justification is required for singling out IP address in this review exercise.

Issue No. 2

To review the regulatory regime for direct marketing activities under section 34 of the Ordinance

Reasons for the Proposal

1. Direct marketing has significant commercial value in promoting the products and prospering the businesses of commercial entities. However, the proliferation of uncontrolled direct marketing activities cause nuisance and annoyance to individuals and encourage the sale of personal data in bulk which infringes the personal data privacy of the data subject, particularly his right "to be let alone".

2. In performing his role, the Commissioner has to balance the benefits to the society at large and the degree of intrusion that the activities have on personal data privacy of individuals. From this perspective, the Commissioner finds it worthy to consider whether to introduce a new requirement that when personal data are used for direct marketing for the first time, the data user shall provide an "opt-in" choice to the data subject.

3. The "opt-in" approach represents a deviation from the present regulatory spirit under section 34, i.e. by allowing the data subject to "opt-out" from the activities instead. The "opt-in" approach has the advantage in that it seeks to obtain the explicit consent of the data subject for so using his or her personal data, which is in alignment with the "prescribed consent" under the use limitation principle expounded under DPP3. An individual's information self-determination is duly respected in this sense. This has also been the approach adopted by some overseas countries.

4. The Unsolicited Electronic Messages Ordinance ("UEM Ordinance"), gives useful insights to the way forward in handling unwelcome calls. Although the UEM Ordinance does not regulate "person to person" calls, automatically generated electronic messages are now tightly governed, such as the sending of spam mails, SMS, unsolicited emails, etc. The UEM Ordinance introduces a central registration system, i.e. the Do-not-Call Register, which contains electronic addresses, the owners of which have expressly indicated their refusal to accept unsolicited electronic messages. The register serves as clear notice and caveat to persons who intend to engage in sending unsolicited electronic messages

not to use the information contained in the register for such purpose.

5. The Commissioner would like to consider the feasibility of following the same approach in setting up a Do-not-Call Register against direct marketing activities so that a data subject can register his contact information to indicate his refusal for using of his personal data by direct marketers. Although the effectiveness of such system introduced under the UEM Ordinance is yet to be seen, the Commissioner would like to solicit views from members of the public and interested groups to ascertain whether a similar system would be desirable to contain the problem of nuisance caused by direct marketing activities.

6. As a means of added protection, the Ordinance may be reviewed to provide a right for the data subject to request disclosure by the direct marketer the source of his personal data collected by it. This will not only prompt for more prudent handling of personal data by data users but will also facilitate the data subject to trace the culpable one who improperly discloses or sells his personal data against the purpose of collection.

The Commissioner's Disposition

Open-minded.

Public Consultation : Recommended or Not

Recommended for the following reason:

The issues touch on the review of the regulatory approach on direct marketing activities and owing to the significant privacy impact that will ensue, voices from different sectors of the society are to be heard before any concrete proposal on amendments can be made.