立法會
Legislative Council

LC Paper No. CB(2)2445/08-09(01)

Ref : CB2/PL/CA

Panel on Constitutional Affairs

Background brief prepared by the Legislative Council Secretariat for the meeting on 11 September 2009

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

Purpose

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

Background

2. The Law Reform Commission (LRC) published a report entitled "Reform of the Law relating to the Protection of Personal Data" in August 1994. Most of the recommendations in the report had been implemented with the enactment of PD(P)O on 3 August 1995. PD(P)O was brought into force on 20 December 1996.

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

The Ordinance

4. PD(P)O protects the privacy of individuals in relation to personal data only. The Ordinance covers any data relating directly or indirectly to a living individual (data subject), from which it is practicable to ascertain the identity of the individual and which are in a form in which access or processing is practicable. It applies to any person (data user) who controls the collection, holding, processing or use of personal data. Data users must follow the fair information practices stipulated in the six data protection principles (DPPs) in Schedule 1 to PD(P)O in relation to the purpose and manner of data collection, accuracy and duration of data retention, use of personal data, security of personal data, availability of data information, and access to personal data.

5. A data user in breach of an enforcement notice is liable to criminal sanction which carries a penalty of a fine at Level 5 (at present $25,001 to $50,000) and imprisonment for two years.

6. PD(P)O gives rights to data subjects. They have the right to confirm with data users whether their personal data are held, to obtain a copy of such data, and to have personal data corrected. Data subjects whose personal data have been compromised may seek damages through civil proceedings; however, there are no statutory provisions or resources at present for PCPD to assist data subjects in claiming damages.

7. PD(P)O shall not apply if the data pertains to an individual whose identity is unknown, or there is no intention to identify that individual. The Ordinance also provides specific exemptions from the requirements of the Ordinance as follows -

(a) a broad exemption from the provisions of the Ordinance for personal data held for domestic or recreational purposes;

(b) exemptions from the requirements on subject access for certain employment related personal data; and

(c) exemptions from the subject access and use limitation requirements of the Ordinance where their application is likely to prejudice certain competing public or social interests, such as security, defence and international relations, prevention or detection of crime, assessment or collection of any tax or duty, news activities, and health.

Review of PD(P)O

8. PCPD formed an internal Ordinance Review Working Group in June 2006 to assess the adequacy of the Ordinance in protecting personal data privacy of individuals. The HA Panel discussed the progress of the review with the Administration and the Privacy Commissioner at its meeting on 4 July 2008. A paper prepared by PCPD on its amendment proposals is in **Appendix I**. While the amendment proposals required further deliberation within the Administration, the Administration had briefed the Panel on its initial thinking in respect of the following proposals put forward by PCPD -

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

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

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

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

9. According to the Administration, a major objective of the comprehensive review of PD(P)O is to examine whether the existing provisions of the Ordinance still afford adequate protection to personal data having regard to developments, including advancement in technology. When considering the proposals put forward by PCPD, the Administration is guided by the following factors -

(a) the Ordinance should provide adequate protection to personal data. However, the right of individuals to privacy is not absolute. It must be balanced against other rights, as well as certain public and social interests and with reference to the particular circumstances they arise;

(b) the need to balance the interests of different sectors/stakeholders;

(c) the need to avoid putting an onerous burden on business operations and individual data users in complying with the requirements of PD(P)O;

(d) perceptions of privacy are dynamic and culture-bound. While there is a need to keep abreast with the development of international privacy laws and standards, due account should be given to local situations;

(e) technology is developing rapidly. To ensure that PD(P)O would remain flexible and relevant in spite of technological change, the provisions in the Ordinance should remain technologically neutral as far as possible; and

(f) a reasonable degree of consensus in the community about the privacy issues is important for providing a stable environment for implementation of the legislation.

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

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

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

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

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

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

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

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

Issues relevant to the review raised by LegCo panels

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

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

14. In accordance with the definition of "personal data" under section 2(1) of PD(P)O, the data must satisfy the requirements of identifiability and retrievability in order to constitute "personal data". "Data" is defined to mean any representation of

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

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

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

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

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

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

there were provisions dealing with the confidentiality of communications made over a public electronic communications network, the use of cookies and the inclusion of personal data in public directories.

Application of PD(P)O

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

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

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

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

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

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

---

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

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

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

Implementation of section 33 of PD(P)O

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

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

Statutory powers and functions of the Privacy Commissioner

24. Arising from a series of incidents relating to leakages of personal data through the Internet and losses of portable electronic storage devices containing such data which involved government bureaux/departments and public as well as private bodies, the ITB Panel discussed issues relating to information security at a number of

---

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

meetings held on 17 March and 11 December 2006, 9 July 2007 and 30 May 2008 respectively. According to the information provided by the Administration for the period from May 2005 to May 2008, the numbers of citizens affected by these incidents were 1 884 for cases occurring in government bureaux/departments and 44 339 for cases occurring in public bodies.

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

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

Reporting and notification arrangements

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

Civil claim for compensation under PD(P)O

28. When consulting the HA Panel on the major recommendations made by LRC on the protection of privacy at its meeting on 9 February 2007, the Administration advised that according to the Report on Civil Liability for Invasion of Privacy, provisions of PD(P)O were concerned only with privacy in relation to personal data, not privacy rights in general. Examples of privacy rights were privacy of the person,

territorial privacy and communications and surveillance privacy. As the Privacy Commissioner did not have the power and resources to provide assistance to aggrieved individuals who wished to make a civil claim under section 66 of PD(P)O, victims who had suffered damage by reason of a contravention of a DPP had to bear all the legal costs unless they were entitled to legal aid. This was contrary to the position of the Equal Opportunities Commission under the Sex Discrimination Ordinance (Cap. 480) (SDO) and the Disability Discrimination Ordinance (Cap. 487) (DDO). LRC therefore recommended in the Report that PD(P)O be amended to enable the Privacy Commissioner to provide legal assistance to data subjects who intended to institute proceedings under section 66 of PD(P)O, along the lines of section 85 of SDO and section 81 of DDO.

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

Relevant questions raised at Council meetings

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

Relevant papers

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

Council Business Division 2
Legislative Council Secretariat
8 September 2009

Appendix I

Review of the Personal Data (Privacy) Ordinance

A decade has passed since the Ordinance came into force on 20 December 1996. The rapid technological and e-commerce developments that are taking place in this electronic era and the exponential rate with which it continues to progress give rise to global privacy concern.

2. Personal data privacy has been an evolving concept responding to changes and development in society. The Commissioner sees the core value of balancing the personal data privacy right with other rights and social interest in maintaining a harmonious society.

3. With a decade of regulatory experience gained in discharge of his 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.

4. With these objectives in mind, an internal Ordinance Review Working Group was formed in June 2006 to assess the adequacy of the Ordinance in protecting personal data privacy of individuals.

5. 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 poses 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.

6. The Commissioner has five missions to achieve in undertaking the review exercise. They are:

(a) To address issues of public concern.
(b) To safeguard personal data privacy rights while protecting public interest.
(c) To enhance the efficacy of regulation under the Ordinance.
(d) To harness matters that will have significant privacy impact.
(e) To deal with technical and necessary amendments.

7. In realizing the above missions, the Commissioner has since then presented to the Secretary for Constitutional and Mainland Affairs a number of amendment proposals and issues of privacy concern. The major proposals are generally described below.

8. Since some of the proposed amendments may have profound impact on data subjects and data users as well as the society at large, it is prudent that these issues are referred to the public for consultation.

(A) To address issues of public concern

I. <u>The leakage of personal data on the internet</u>

A series of incidents relating to leakage or loss of sensitive personal data cause privacy concern, for instance, the IPCC leakage of complainants'

personal data, on-line dissemination of the nude photos and the loss of patients' data by the Hospital Authority. While there are at present provisions under the Ordinance regulating data users in safeguarding data security, the Commissioner finds that it is timely to strengthen the provisions to enhance the protection of personal data privacy in the following manner:

(a) In order to curb irresponsible dissemination of leaked personal data, he proposes to make it an offence for any person who knowingly or recklessly, without the consent of the data user, obtains or discloses personal data held or leaked by the data user. It is also proposed to make it illegal the subsequent selling of the personal data so obtained for profits. Such a legislative approach is similar to section 55 of the Data Protection Act in the UK which has been in force for more than seven years. An offence under this section is currently punishable by a fine of up to £5,000 in a Magistrates' court or an unlimited fine in the Crown Court. Legislation to introduce the possibility of a custodian sentence is now before UK Parliament. The Commissioner notes the increasing invasion of personal data privacy posed by the overwhelming technological advances. Hong Kong will be seen to be regressing in its effort to protect data privacy if the Ordinance does not keep pace with changes and development that are taking place.

(b) In relation to the transfer of personal data to an outsourced agent or contractor for handling, he proposes that consideration be given (i) to impose new obligation on the data user when engaging processing agent; and (ii) to require the processing agent to observe the requirements of the Ordinance.

(c) In order to mitigate or reduce the damages that may cause the data subjects whose personal data are leaked or lost, he proposes that consideration be given whether or not to introduce mandatory privacy breach notification requirement. Under this proposal, the data user shall promptly notify individuals affected by the loss or theft of personal data in certain breaches where there was a high risk of significant harm. The Commissioner's Office should also be notified upon happening of the relevant

events.

II. The disclosure of personal data by internet or email service providers

The Yahoo's case[1] has revealed some grey areas under the Ordinance which the Commissioner in his investigation report of the case has promised to review. He proposes:

(a) to consult the public as to whether the definition of "personal data" should be broadened to deem IP address as "personal data";

(b) to give a meaning to the word "crime" under the Ordinance;

(c) to clarify the extent of application of the Ordinance where none of the acts of the data processing cycle takes place in Hong Kong.

III. The handling of personal data in time of crisis

It was recounted that in the horrendous South Asian tsunami happened in 2004, difficulties were encountered in disclosing location or contact data of the missing persons by the relevant government departments to assist family members of the missing persons. There was no exemption provision under the Ordinance that could be safely invoked and relied upon. To address this aspect, the Commissioner proposes to amend the Ordinance to deal with the use of personal data when there is overriding public interest, particularly in emergency situation.

(B) Safeguarding personal data privacy rights while protecting public interest

In achieving the above mission, the Commissioner has duly considered the following in the course of the review:

(a) While noting the commercial value of direct marketing activities, the Commissioner sees the need to curb unwelcome calls and nuisances to the recipients of the direct marketing calls. He

[1] See report published, available at (http://www.pcpd.org.hk/english/publications/files/Yahoo_e.pdf) and the decision of Administrative Appeals Board in AAB No.16/2007, available at (http://www.pcpd.org.hk/english/publications/files/Appeal_Yahoo.pdf).

proposes that public consultation be carried out to scrutinize alternative proposals in regulating the activities.

(b) The rationale for granting exemptions under the Ordinance is motivated by the need to balance different and, usually, conflicting interests. There are situations that public and social interests are so overwhelming or where the benefits to be obtained by the data subject substantially outweigh the degree of intrusion into his personal data privacy that a case for exemption is made out. The Commissioner makes a number of proposals in this respect.

(c) The Commissioner has received submissions from organizational data users the practical difficulties in complying with data access requests. In his proposals for amendment, he makes clear the duty of a data subject to make specific data access request and addresses certain comments made by the Administrative Appeals Board on the data access provisions of the Ordinance.

(C) Enhancing efficacy of regulation under the Ordinance

I. <u>Reviewing investigation procedures</u>

For efficient utilization of his limited resources to better perform his regulatory role, the Commissioner finds it necessary to have express power to conduct preliminary enquiry. Additional grounds of refusal to carry out or continue an investigation are proposed and that the Commissioner should be conferred with a specific power to discontinue an investigation at any time.

II. <u>Effective enforcement</u>

The Commissioner finds it more efficient and cost effective for him to undertake criminal investigation and prosecution. In addition, it will validate the independence status of the Commissioner as the regulator of both the public and private sectors.

It follows that incidental powers conducive to the carrying out of the aforesaid function should be provided. Moreover, the current time bar for

prosecution should be extended. To strengthen enforcement actions, the Commissioner proposes to relax the current criteria for issuance of an enforcement notice. Additional offence provisions and heavier penalties are introduced in order to serve as an effective deterrent.

III. Consent given by individuals

Sometimes, the data subject does not have a sufficient understanding of what is proposed to him for consent owing to age or mental incapacity. The Commissioner makes proposal to address the problem so that upon meeting specified criteria, "prescribed consent" made by another person shall be deemed as good as the one obtained from the data subject.

IV. Data access request

The Commissioner has received submissions from social workers about the making of data access requests by parents for their children's personal data which the children have specifically objected to release. To address the concern, the Commissioner makes proposal on respecting the privacy right of children.

(D) Harnessing matters that will have significant privacy impact

The Ordinance as it currently stands does not contain provisions differentiating personal data that are "sensitive" from those that are not. According to international practice and standards, certain kinds of personal data are regarded as inherently sensitive, e.g. one's 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. 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, where the collection is required by law, or where the collection is necessary to prevent or lessen a threat to the life or health of an individual.

The case for treating certain personal data as sensitive are as follows :

(i) It is consistent with the legislative intent to provide a higher degree

of protection towards more sensitive personal data. In particular, under Data Protection Principle 4, 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[2], thereby enabling the Ordinance to pass the EU adequacy test on personal data protection.

(E) Technical and necessary amendments

There are technical issues found in the Ordinance that require improvements in order to quell any doubt, rectify any error, omission, inconsistency and uncertainty. For instance, it should be sufficient for the data user to discharge its notification duty under Data Protection Principle 1(3)(b)(ii)(B) by giving the job title and the address of the individual to whom a data access and correction request may be made. Moreover, the Commissioner and his prescribed officers should be immune from suit when acting in good faith in exercising the functions and powers under the Ordinance.

---

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on *the Protection of individuals with regard to the Processing of Personal Data and on the Free Movement of such Data*, available at (http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett)

It is also desirable for the Commissioner to be exempted from the duty of secrecy under section 46 when disclosing information reasonably for the proper performance of his functions and the exercise of his powers under the Ordinance.

Some issues of privacy concern

9. The Commissioner is also mindful of an inoperative provision under the Ordinance which is section 33 concerning the prohibition against transfer of personal data to a place outside Hong Kong. Meanwhile, e-commerce and transborder data flow of personal data are the order of the day and continue to prosper. The Commissioner, though being ready to do so, has not yet specified under section 33(3) a "white list" of overseas countries or regions that afford comparable personal data privacy protection as Hong Kong.

10. The Data User Registration Scheme under Part IV of the Ordinance (which has yet to be implemented) requires a data user to give the names or description of the places outside Hong Kong to which the data user transfers, intends to transfer or may wish to transfer personal data. The transparency of the registration system will be beneficial for making known the acts and practices of the data users for better guidance to data subjects.

11. Time is ripe now for a review to be undertaken to bring closer the operation of section 33. The Commissioner would like to solicit the views and responses as to whether the society is now ready for bringing into force section 33 and if not, the criteria for consideration and determination in future.

Conclusion

12. The Commissioner is confident that a comprehensive review of the Ordinance with participation by the general public will bring about an updated piece of privacy legislation that amply protects and enforces personal data privacy right in Hong Kong.

Office of the Privacy Commissioner for Personal Data
June 2008

Appendix II

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

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

Meeting Date	Question
21.5.08	Hon Emily LAU raised a written question on the review of the Personal Data (Privacy) Ordinance.
26.11.08	Hon CHEUNG Hok-ming raised a written question on whether the unauthorized disclosure of personal data by credit card-issuing bodies to debt collection agencies had contravened provisions of the Personal Data (Privacy) Ordinance.

Council Business Division 2
Legislative Council Secretariat
8 September 2009

Appendix III

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

Relevant documents

Meeting	**Meeting date/ publication date**	**Paper**
--	August 1994	Report entitled "Reform of the Law Relating to the Protection of Personal Data" published by Law Reform Commission
Financial Affairs Panel	24 September 2002	Consultation document issued by the Office of the Privacy Commissioner for Personal Data on the Proposed Provisions on Consumer Credit Data Protection: the Sharing of Positive Credit Data [LC Paper No. CB(1)2454/01-02(01)] Paper from the Office of the Privacy Commissioner for Personal Data on "Consultation Document on the Proposed Provisions on Consumer Credit Data Protection: the Sharing of Positive Credit Data" [LC Paper No. CB(1)2558/01-02(02)] Minutes of meeting [LC Paper No. CB(1)281/02-03] Report on the Public Consultation in relation to the Sharing of Positive Credit Data: Proposed Provisions on Consumer Credit Data Protection; and the related press release provided by the Office of the Privacy Commissioner for Personal Data [LC Paper No. CB(1)806/02-03]
Panel on Information Technology and Broadcasting (ITB Panel)	1 November 2005	Submission from the Office of the Privacy Commissioner for Personal Data on Issues related to the Protection of Personal Information of E-mail Account Subscribers [LC Paper No. CB(1)160/05-06(01)] Administration's paper on "Licensing Framework for Internet Service Providers and Protection of Personal Data" [LC Paper No. CB(1)173/05-06(01)]

Meeting	**Meeting date/ publication date**	**Paper**
		Speaking note of the Privacy Commissioner for Personal Data [LC Paper No. CB(1)211/05-06(01)] Minutes of meeting [LC Paper No. CB(1)412/05-06] Letter dated 28 October 2005 from Yahoo! Holdings (Hong Kong) Limited to the Chairman of ITB Panel [LC Paper No. CB(1)186/05-06(03)] Paper prepared by the Legal Service Division on scope of "Personal Data" under the Personal Data (Privacy) Ordinance (Cap. 486) and related issues [LC Paper No. LS21/05-06] Report of the Office of the Privacy Commissioner for Personal Data published under Section 48(2) of the Personal Data (Privacy) Ordinance (Cap. 486) [LC Paper No. CB(1)1233/06-07(01)]
Home Affairs Panel (HA Panel)	8 November 2005	Minutes of meeting [LC Paper No. CB(2)577/05-06]
ITB Panel	17 March 2006	Submission from the Office of the Privacy Commissioner for Personal Data on Information Security [LC Paper No. CB(1)1093/05-06(02)] Administration's paper on "Information Security" [LC Paper No. CB(1)1097/05-06(01)] Minutes of meeting [LC Paper No. CB(1)1382/05-06]
	11 December 2006	Administration's paper on "Information Security" [LC Paper No. CB(1)435/06-07(05)]

Meeting	**Meeting date/ publication date**	**Paper**
		Background brief on Information Security [LC Paper No. CB(1)435/06-07(06)] Minutes of meeting [LC Paper No. CB(1)669/06-07]
HA Panel	9 February 2007	Report on Civil Liability for Invasion of Privacy published by Law Reform Commission in December 2004 Administration's paper on "Protection of Privacy" [LC Paper No. CB(2)1014/06-07(01)] Background brief on Reports published by the Law Reform Commission on privacy [LC Paper No. CB(2)1014/06-07(02)] Minutes of meeting [LC Paper No. CB(2)1501/06-07]
ITB Panel	9 July 2007	Administration's paper on "Information Security" [LC Paper No. CB(1)2034/06-07(04)] Updated background brief on Information Security [LC Paper No. CB(1)2063/06-07(01)] Minutes of meeting [LC Paper No. CB(1)2396/06-07]
	30 May 2008	Administration's paper on "Information Security" [LC Paper No. CB(1)1679/07-08(01)] Administration's paper on "Data leakage incidents involving various bureaux/ departments for the last 3 years up to 22 May 2008 [LC Paper No. CB(1)1875/07-08(01)] Minutes of meeting [LC Paper No. CB(1)2311/07-08]

Meeting	**Meeting date/ publication date**	**Paper**
HA Panel	4 July 2008	Administration's paper on "Review of the Personal Data (Privacy) Ordinance" [LC Paper No. CB(2)2488/07-08(01)] Administration's paper on "Protection of Personal Data Privacy" [LC Paper No. CB(2)2454/07-08(01)] Speaking note of the Privacy Commissioner for Personal Data [LC Paper No. CB(2)2528/07-08(01)] Information note on "Implementation problems of the Personal Data (Privacy) Ordinance" prepared by Research and Library Services Division of the Legislative Council Secretariat [LC Paper No. IN21/07-08] Minutes of meeting [LC Paper No. CB(2)2850/07-08]
Constitutional Affairs Panel	23 October 2008	Administration's paper on "2008-09 Policy Agenda" [LC Paper No. CB(2)72/08-09(01)]

Council Business Division 2
Legislative Council Secretariat
8 September 2009