Legislative Council Panel on Home Affairs

Review of the Personal Data (Privacy) Ordinance

Purpose

The Administration is conducting a comprehensive review of the Personal Data (Privacy) Ordinance (PDPO) in conjunction with the Office of the Privacy Commissioner for Personal Data (PCPD). This paper informs members of the progress of the PDPO review.

Background

2. The PDPO was enacted in 1995 to achieve two goals, namely, to ensure proper protection of an individual's right to privacy with regard to personal data, and to obviate the risk of restrictions imposed by other countries on the free flow of personal data to Hong Kong. The Ordinance took forward the majority of the recommendations of the Law Reform Commission Report on Reform of the Law Relating to the Protection of Personal Data released in August 1994, which was based on more than four years of work, including a thorough public consultation exercise.

3. The PCPD started an internal review of the PDPO in June 2006 to assess the adequacy of the Ordinance in protecting personal data privacy of individuals. The Administration is discussing the various amendment proposals with the PCPD.

The Review

4. A major objective of the comprehensive review of the PDPO 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, in the last decade. When considering the proposals by the PCPD, we are guided by the following :

(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 onerous burden on business operations

and individual data users in complying with the requirements of the PDPO;

(d) perceptions of privacy are dynamic and culture-bound. While we see 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 the PDPO 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.

5. At the Annex is a paper prepared by the PCPD on its amendment proposals. We are working with the PCPD to assess the feasibility and impact of the various proposals. In doing so, we will take into consideration the factors mentioned in paragraph 4 above. A number of the proposals may have an impact on the relevant economic sectors and the community at large. Some examples are outlined in the following paragraphs.

Sensitive Personal Data

6. At present, the PDPO does not contain provisions which differentiate personal data that are "sensitive" from those that are not. In line with international practice and standards, the PCPD proposes to provide a higher degree of protection towards sensitive personal data to safeguard against indiscriminate and improper handling. Such data could include racial or ethnic origin, political affiliation, religious beliefs, membership of trade unions, physical or mental health, biometric data and sexual life. The idea is that handling of sensitive personal data is prohibited unless specified circumstances are met, such as where there is explicit consent from the data subject, collection of data is necessary to protect the vital interests of the data subject or another person, or it is required by law. Contravention of the prohibition will be made an offence under the PDPO.

7. What constitutes sensitive personal data would need to be fully deliberated by the community as perception of sensitive personal data is culture-bound. We also need to consider the circumstances under which processing of sensitive personal data are allowed, and the penalties for

breach of the requirements of handling sensitive personal data.

Direct Prosecution Power

8. At present, the PDPO confers the Privacy Commissioner with powers of investigation and inspection. However, the Commissioner cannot initiate prosecution. Criminal investigations are conducted by the Police and prosecutions, where there is sufficient evidence, by the Department of Justice. The PCPD proposes that the Privacy Commissioner be vested with direct prosecution power.

9. Under the Basic Law, the control of criminal prosecutions is vested in the Department of Justice. In considering whether this prerogative should be delegated, we will consider the justification, the circumstances under which the power could be delegated, overseas practice, the practices under other local ordinances and the availability of alternatives.

Criminalisation

10. At present, a contravention of a data protection principle (DPP) is not an offence. It is only upon the breach of an enforcement notice issued after the completion of an investigation that the relevant data user is liable to criminal sanction. The PCPD has conducted a comparative study of overseas data protection legislation and found the current provisions of the PDPO to be in line with international jurisprudence on personal data privacy legislation. However, the PCPD considers that making a contravention of any DPP a criminal offence would have a significant impact on civil liberties in that a data user may incur criminal liability for an inadvertent act or omission.

11. Having regard to the above considerations, the PCPD proposes that we should focus on particular acts or practices which should be singled out as criminal offence to achieve deterrent effect and better protect the personal data privacy of individuals. These include, for example, 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; and repeated infringement of the requirements of the PDPO on similar facts.

12. The Administration considers that proposals on criminalization would affect the community at large, and in particular data users and members of the public. Before taking a view on the way forward, we will need to study the proposals carefully, taking into account the need to strike a balance between protection of personal data privacy and other human rights.

Penalty Level

13. At present, the maximum penalty for contravention of the PDPO is a fine at level 5 ($50,000) and imprisonment for two years. The PCPD proposes to raise the penalty level for certain acts of contraventions, such as a second or subsequent breach of an enforcement notice.

14. The Administration considers that any proposed penalty level should be mapped out having regard to the penalty levels under the PDPO in terms of relativity and proportionality. We will look into the penalties under the PDPO as a whole, having due regard to the severity of the contravening acts, the desired deterrent effect, the proportionality between the punishment and the harm caused to an individual, and the relative importance of the personal data privacy rights that the PDPO seeks to protect.

Way Forward

15. The review of the PDPO covers fundamental issues which affect the rights and civil liberties of individuals. The proposals will impact on various sectors of the community, public and private organizations and members of the public. We see a need to carefully examine and thoroughly deliberate the various issues before the Administration comes up with its proposals to amend the PDPO. After the Administration has undertaken a more detailed assessment of the implications of the amendment proposals, we will consult the public before determining the way forward.

Views Sought

16. Members are invited to note the content of this paper.

June 2008
Constitutional and Mainland Affairs Bureau

Annex

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