Paper for Legislative Council
Panel on Information Technology and Broadcasting
Meeting to be held on 17 March 2006

Agenda Item IV – Information Security

Reported incidents of leakage on the Internet of personal information held by the Independent Police Complaints Council ("IPCC") and some other private organizations

Introduction

The recently reported incidents of leakage on the Internet of complainants' personal data held by IPCC and customers' personal data held by a telecommunications operator and an insurance company raised public concerns over the security of personal data.

2. In discharge of his functions and duties under the Personal Data (Privacy) Ordinance, Cap 486 ("the Ordinance"), immediate actions have been taken by the Privacy Commissioner for Personal Data ("the Commissioner"). He has approached the IPCC and made enquiries on the circumstances leading to this incident. Since the reporting of the incident, the Commissioner's Office has received 6 complaints on the subject matter. The Commissioner's Office will continue to handle the cases in accordance with its Complaint Handling Procedures in pursuance of which an investigation will be carried out where a *prima facie* case of contravention of the requirement of the Ordinance is found.

3. With respect to other cases of suspected leakage of customers' personal data by a telecommunications operator and an insurance company reported by the media, the Commissioner is now making enquiries with the parties concerned. Self-initiated investigation will be carried out where *prima facie* case exists.

Statutory provisions on protection of personal data

4. Of relevance to the security of personal data is the requirement under

Data Protection Principle ("DPP") 4 in Schedule 1 to the Ordinance. It provides as follows:-

> *"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."*

The word "practicable" is further defined under section 2(1) of the Ordinance as meaning "reasonably practicable".

5. In the electronic age, data security is a serious concern as electronic data can be copied, reproduced and transferred on the Internet within seconds. In the case of electronic storage of substantial amount of sensitive personal data, an enhanced level of security is needed to guard against unauthorized or accidental access, processing or other use.

6. Other requirements that are of relevance to leakage of personal data on the Internet are DPP1 and DPP3. In accordance with DPP1, personal data shall only be collected for a lawful purpose directly related to the data user's function or activity and the personal data collected should be necessary, adequate but not excessive. The means of collection shall be lawful and fair in the circumstances of the case. As for DPP3, it provides that personal data shall only be used for the purposes for which they were originally collected or a directly related purpose unless the prescribed consent of the data subject is obtained. Personal data contained in the IPCC database is for internal use only. Any illegal collection from the Internet or subsequent use of such data will be in breach of DPP1 and/or DPP3 of the Ordinance.

Enforcement actions under the Ordinance

7. Although section 4 of the Ordinance requires compliance of the data protection principles by a data user, the Ordinance does not provide for breach of a data protection principle itself (unless reinforced with a corresponding provision of the Ordinance, such as, failure to comply with a data access request under section 19 or non-erasure of personal data no longer required under section 26) to amount to an offence. Where the Commissioner finds a contravention of the data protection principle upon investigation, an enforcement notice may only be issued under section 50 when the data user is contravening or has contravened a requirement under the Ordinance in circumstances that it will continue or be repeated. When the breach of the data protection principle appears in the circumstances of the case to be a single incident unlikely to be repeated, the Commissioner shall not issue an enforcement notice although he may instead issue a warning against the data user.

8. The enforcement notice will direct the data user to take steps to remedy the contravention and if it is not complied with, the data user commits an offence under section 64(7) punishable with a fine at level 5 (i.e. $50,000) and imprisonment for 2 years and in the case of a continuing offence, to a daily penalty of $1,000. Since the Commissioner is not yet equipped with prosecution powers, if a data user is found to have failed to comply with an enforcement notice, the Commissioner can only refer the case to the Hong Kong Police for investigation and for taking prosecution action by the Department of Justice under section 64(7) where appropriate.

9. Upon completion of an investigation, the Commissioner may also publish a report pursuant to section 48(2) of the Ordinance if he is of the opinion that it is in the public interest to do so. The report will set out the results of the investigation and the recommendations or comments arising from the investigation. In the report, he may disclose the identity of the relevant data user. However, before publication of the report, he has to supply a copy of the report to the relevant data user inviting it to advise in writing within 28 days whether in the opinion of the data user there is any matter in the report which would involve the disclosure of personal data that are exempt from the provisions of DPP6 by virtue of an exemption under Part VIII of the Ordinance. The report may only be published if the Commissioner receives no such

objection to disclosure of information or he accepts the objection and delete the relevant information. In the event that the Commissioner refuses to delete the relevant information, the relevant data user has a right of appeal to the Administrative Appeals Board.

Other proactive steps that the Commissioner may take

10. The Commissioner is also empowered under the Ordinance to take proactive steps to ensure compliance with the requirements of the Ordinance such as by carrying out compliance check from time to time or exercising his powers of inspection on any personal data system pursuant to section 36 of the Ordinance. He may also take the initiative to carry out an investigation in the absence of a complaint under section 38(b) when he has reasonable grounds to believe that there may be a contravention by the data user of the requirement of the Ordinance.

11. For better protection of personal data against improper use or handling and to allay the data subjects' privacy concerns arising from this unfortunate incident, the Commissioner is actively considering the launching of the data user returns for a register of data users to be kept with the Commissioner so that the public can access and search for the prescribed information about personal data collected held and processed by the data user. It is anticipated that the project be launched in phases to eventually cover all classes of data users.

Civil remedies under the Ordinance

12. Any individual who suffers damage, including injury to feelings, from contravention of the requirement of the Ordinance is entitled to file civil suit under section 66 of the Ordinance to claim for damages.

Review of the Ordinance

13. The present scheme under the Ordinance is not to make it a direct offence for infringement of the DPPs. It is only upon the issuance of an enforcement notice (the issuance of which is predicated upon the contravention is continuing or likely to be repeated) and the failure to comply with the terms of the enforcement notice that an offence will be committed. That explains

the reason why over the years, the number of prosecution cases taken under the Ordinance is low. It appears that the legislative intent is not to impose serious punishment since protection of privacy right is customarily a new concept when introduced in the 1990s. Now that the Ordinance has been in force for nearly a decade, it is time to review whether more serious punishment should be imposed on infringement of the Ordinance and whether the Commissioner should be conferred with criminal investigation and prosecution powers.

Office of the Privacy Commissioner for Personal Data
16 March 2006

u:kitty/kcmisc/Legco panel on 17 Mar 2006 (Eng).doc