

---

---

## INFORMATION NOTE

### Implementation problems of the Personal Data (Privacy) Ordinance

#### 1. Background

1.1 At the meeting of the Panel on Home Affairs (the Panel) on 11 October 2007, the Panel requested the Research and Library Services Division (RLSD) to prepare a paper about public views on the implementation problems of the Personal Data (Privacy) Ordinance<sup>1</sup> (Cap. 486) (Ordinance) to facilitate the deliberation of the issue by the Panel.

1.2 In this research, RLSD studied the publicly available information, including the relevant Legislative Council papers, local press reports published between 4 December 2004 and 25 June 2008, and materials on the website of the Privacy Commissioner for Personal Data Office (Office). In addition, RLSD asked the Office to provide inputs on the implementation problems of the Ordinance and recommendations to improve the effectiveness of implementing the Ordinance.

1.3 Based on the research materials studied, the implementation problems of the Ordinance may be categorized into the following six aspects:

- (a) lack of prosecution power;
- (b) contravention of data protection principles;
- (c) protection of personal data;
- (d) protection of personal information of e-mail account subscribers;
- (e) transfer of personal data; and
- (f) other issues.

---

<sup>1</sup> Please see Appendix I for some basic information on the Ordinance.

## 2. Implementation problems of the Ordinance

### Lack of prosecution power

#### *Public views*

2.1 One of the implementation problems of the Ordinance is that the Privacy Commissioner for Personal Data (Commissioner) is not empowered to institute prosecutions directly against those whom are determined after the Office's investigation to have contravened the Ordinance. Instead, the Commissioner is required to refer and explain those cases to the police for a second investigation and then to the Department of Justice for prosecution. Further, prosecution of offences under the Ordinance is required to be instituted within six months of the Commissioner's knowledge. Under such circumstances, very few cases have been convicted of contravening the Ordinance since its enactment. As such, the Commissioner has been labelled in some local press reports as a "toothless tiger".

#### *The Commissioner's view*

2.2 The Commissioner shares the public views that he lacks the necessary power to carry out criminal investigation, seize exhibits and prosecute an offence. In fact, he has been asking the Government to expand his power for prosecution.<sup>2</sup>

### Contravention of data protection principles

#### *Public views*

2.3 Under the Ordinance, the Commissioner is not empowered to institute prosecutions directly against those who have contravened data protection principles, which are set out in Schedule 1 to the Ordinance.<sup>3</sup> There are discussions on whether the contravention of data protection principles should be made an offence. There is concern as revealed in some local press reports that making non-compliance with the data protection principles an offence may have an impact on civil liberty as a data user may face criminal liability for an inadvertent act or omission.

---

<sup>2</sup> A proposal containing more than 50 recommendations was drawn up and submitted by the Commissioner to the Government in December 2007, calling for a public consultation and amendments to the Ordinance. The Government responded that it would conduct a comprehensive review of the Ordinance with the Commissioner. The review would examine ways to further strengthen protection on personal data privacy with regard to the collection, holding, processing and use of personal data.

<sup>3</sup> Please see paragraphs A.I.4 and A.I.5 of Appendix I for details of data protection principles.

*The Commissioner's view*

2.4 According to the Commissioner, some members of the public may not know that contravention of data protection principles is not an offence per se. It is only upon the breach of an enforcement notice issued after completion of a formal investigation that the relevant data user is liable for criminal prosecution. The current criteria for issuance of an enforcement notice are considered by the Commissioner as overly restrictive in that the Commissioner may serve an enforcement notice only when a contravention is likely to continue or be repeated.

Protection of personal data*Public views*

2.5 In view of the occurrence of many personal data leakage incidents in the past few years<sup>4</sup>, many members of the public have expressed that the Ordinance may need to be reviewed and improved to better protect personal data. In many cases, the leakage of personal data may cause damage, distress or embarrassment to the individuals concerned. Many members of the public consider that the Ordinance should ensure data users have a responsibility to safeguard the security of personal data.

2.6 In particular, some members of the public have proposed that:

- (a) in case of personal data leakage, the data users concerned should notify the affected persons, the Commissioner<sup>5</sup>, the relevant trade regulators and the relevant government bureaux/departments as soon as possible;
- (b) the Commissioner should consider assisting the affected persons to seek compensation from the data users concerned for the damages through civil proceedings;

---

<sup>4</sup> See Appendix II and Appendix III for details. Appendix II gives a brief account of an incident of personal data leakage relating to complaints made against the police by the public on the Internet. Such data were held by the Independent Police Complaints Council. Appendix III highlights selected incidents relating to the leakage of personal data held by various institutions. These incidents had caused serious public concern.

<sup>5</sup> Under the Ordinance, data users are not required to report leakage of personal data to the Commissioner.

- 
- 
- (c) in view of the recent incidents of leakage of personal data by government bureaux/departments and public bodies<sup>6</sup>, the Government should consider enacting laws on the management of government records to specify clearly the authority of and restrictions on government bureaux/departments and public bodies in handling personal data; and
  - (d) the Commissioner should allocate more resources educating civil servants, businessmen and the public with a view to raising their awareness of personal data protection and reminding them of the need to comply with the Ordinance, relevant guidelines and codes of practice.

#### *The Commissioner's view*

2.7 According to the Commissioner, the incidents of personal data leakage have demonstrated clearly to the Government that there is a pressing need to actively consider amending the Ordinance to better protect the public interest.

2.8 In particular, he has proposed to create a new offence for knowingly, without the consent of a data user, obtaining or disclosing personal data held or leaked by the data user or the selling of personal data so obtained. This can serve as an effective deterrent in sanctioning irresponsible behaviour in handling personal data online.

2.9 As said, under the current provisions of the Ordinance, contravention of a data protection principle does not cause criminal sanction. There exists a loophole which allows a person who, in flagrant disregard of the personal data privacy of the original data user, can sell or trade in personal data collected without consent or personal data which have been leaked.

2.10 Two cases have been provided by the Commissioner where personal data privacy is abused:

- (a) an unauthorized access to 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; and

---

<sup>6</sup> Based on the Government's figures, in the past three years up to 22 May 2008, there were 14 incidents involving the leakage of personal data of around 1 900 citizens reported by government bureaux/departments. During the same period, there were 16 cases of personal data leakage incidents occurred in public organizations involving about 44 000 citizens. According to the Government, most of the incidents were caused by lack of awareness of information security policies and guidelines, especially on the use of portable storage devices and file-sharing software. In this connection, the Government would review its policies on information security in the next few months.

- 
- 
- (b) the use of personal data for personal gains of the collector, such as the sale of the data to direct marketing companies or for perpetuating crime by theft of identity.

2.11 According to the Commissioner, when considering introducing appropriate sanction measures, Hong Kong may make reference to the experience of the United Kingdom (UK). In the UK, personal data protection is provided under section 55 of the Data Protection Act which came into force in March 2000. The Act makes it an offence (with certain exemptions<sup>7</sup>) to obtain, disclose or procure the disclosure of personal information knowingly or recklessly, without the consent of the data user and fine as penalty was imposed. Based on the figures provided by the UK Information Commissioner's Office, some 1 000 complaints relating to section 55 of the Act were received in the six years since the enactment of the Act. A total of 25 prosecutions was brought between mid-November 2002 and January 2006, which nearly all resulted in convictions.

#### Protection of personal information of e-mail account subscribers

##### *Public views*

2.12 In the wake of the case of Mr Shi Tao<sup>8</sup>, some members of the public have expressed that a review of the Ordinance should be conducted on whether Internet Protocol (IP) addresses should be regarded as a type of "personal data"<sup>9</sup> so that such information can be protected under the Ordinance.

##### *The Commissioner's view*

2.13 In light of the public concern on the protection of personal information of e-mail account subscribers, the Commissioner has stated that there are two "technical" aspects of the Ordinance needed to be clarified:

- (a) whether the Ordinance should apply where none of the act of collecting, holding, processing and using of personal data takes place in Hong Kong; and
- (b) whether the Ordinance should apply where the disclosure of personal data is made in compliance with a lawful order issued by a foreign authority under foreign law for the purpose of investigation of a foreign crime.

---

<sup>7</sup> Some of the exemptions include: (a) preventing or detecting crime and (b) protecting the public interest.

<sup>8</sup> See Appendix IV for some basic information about the case of Mr Shi Tao.

<sup>9</sup> According to the Commissioner, an IP address alone does not satisfy the definition of "personal data" in the Ordinance. However, if the IP address is combined with identifying particulars of an individual, from which it is practicable for the identity of the individual to be ascertained, the IP address may become part of "personal data".

2.14 To this end, he considers that the Ordinance should be amended to provide a clearer interpretation and application of the Ordinance so as to enhance the overall effectiveness in the protection of personal data privacy.

### Transfer of personal data

#### *Public views*

2.15 Section 33 of the Ordinance prohibits the transfer of personal data from Hong Kong to places that do not have adequate data protection legislation. However, this provision of the Ordinance has not yet been in operation. It has been reported that the Government and the Commissioner are co-working to draft the relevant guidelines and suitable model contracts to be entered into by data users and data transferees.

2.16 As the commencement of the operation of section 33 would have implications on trans-border data transfer activities of various business sectors, notably the banking and telecommunications sectors, the Government and the Commissioner may need to map out the best way forward, taking into account the interests of relevant stakeholders.

#### *The Commissioner's view*

2.17 The Commissioner has opined that there is no explicit provision in the Ordinance to allow a transfer of personal data in business merging or acquisition. Hence, this may be one aspect of the Ordinance which needs to be reviewed.

### Other issues

2.18 The Commissioner has identified the following implementation problems of the Ordinance and suggested recommendations to improve the effectiveness of implementing the Ordinance.

#### *Data users registration scheme*

2.19 Under section 14 of the Ordinance, the Commissioner has the discretionary power to specify classes of data users required to submit data user declarations. There shall be a data user registration scheme to allow data subjects to know:

- (a) the sort of personal information data users hold;

- (b) for what purpose(s) they hold the information; and
- (c) how they collect, hold, use and disclose personal data to third parties.

2.20 However, this statutory requirement has not been put into effect. The Commissioner has proposed that data users should be required to register with the Office and explain why they are collecting information on people. The requirement of registering with the Office would force organizations to be more open and transparent. When investigating a complaint, privacy officers would be able to refer to the registration information to find out if the data is being used for reasons other than that provided on the registration form.

#### *Lack of resources*

2.21 The Commissioner has stated that given the Office's limited resources, he has to fulfil his statutory functions and meet the public expectation of protecting personal privacy. In 2008-2009, he could only allocate HK\$600,000 towards promoting awareness and understanding of the Ordinance. To carry out effectively this aspect of his statutory functions, a substantial increase in resources is needed.

2.22 In addition, technological development creates challenges in various security aspects, which include:

- (a) releasing one's own personal data to unknown individuals and on unknown websites; and
- (b) leaking personal data on the Internet.

2.23 In terms of technological support, the Commissioner has only one officer established in his Office to render day-to-day support and none in terms of ensuring compliance of the Ordinance by data users.

2.24 The Commissioner has also stated that he was unable to exercise his inspection power under section 36 of the Ordinance<sup>10</sup> due to lack of funds. His limited resources have to be applied in the handling of complaint cases and compliance checks arising out of reported privacy breaches. However, in view of the series of incidents on the loss of patients' personal data by various hospitals and clinics which has caused serious concern of the public and the Commissioner, the Commissioner has exercised his inspection power for the first time to carry out an inspection on the personal data systems used by a data user (the Hospital Authority).

*Recommendations to improve the effectiveness of implementing the Ordinance*

2.25 The Commissioner has stated that there have not been any amendments to the Ordinance since its enactment in 1996. On the other hand, international data protection authorities are proposing tougher legislation and adopting more proactive approaches and initiatives in conducting compliance investigations (in the absence of a complainant), privacy impact assessments on new projects and privacy audits on existing projects that collect and process a substantial amount of personal data.

2.26 During the past two years, the Commissioner has been reviewing the entire Ordinance (particularly on addressing the implementation problems) and considering various measures to bring it on par with overseas data protection legislation, so that Hong Kong does not suffer from a want of information flow and overseas business opportunities as a result of inadequacies in the domestic legislation.

2.27 To improve the protection of privacy in Hong Kong, the Commissioner has proposed a public consultation exercise with a view to introducing more robust protection of personal data privacy.

---

Prepared by Jackie WU  
27 June 2008  
Tel: 2869 9644

---

*Information notes are compiled for Members and Committees of the Legislative Council. They are not legal or other professional advice and shall not be relied on as such. Information notes are subject to copyright owned by the Legislative Council Commission (the Commission). The Commission permits accurate reproduction of the information notes for non-commercial use in a manner not adversely affecting the Legislative Council, provided that acknowledgement is made stating the Research and Library Services Division of the Legislative Council Secretariat as the source and one copy of the reproduction is sent to the Legislative Council Library.*

---

<sup>10</sup> Under section 36 of the Ordinance, the Commissioner is empowered to conduct on-site privacy checks to "walk through the personal data system" used by a data user or a group of data users. Prevention of data breaches is the primary objective of the inspection. Upon completion of an inspection, the Commissioner shall inform the relevant data user of the result of the inspection and make recommendations to facilitate compliance with the Ordinance.

## Appendix I

### Some basic information on the Personal Data (Privacy) Ordinance

#### Commencement of the Ordinance

A.I.1 The Personal Data (Privacy) Ordinance (Ordinance) (Cap. 486) was brought into force on 20 December 1996.

#### Objectives

A.I.2 One objective of the Ordinance is to protect the privacy interests of living individuals in relation to personal data. It also contributes to Hong Kong's continued economic well being by ensuring a free flow of personal data to Hong Kong from places that already have data protection laws.

#### Scope of coverage

A.I.3 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.

#### Implications for data users and data subjects

A.I.4 Data users must follow the fair information practices stipulated in the six data protection principles in Schedule 1 to the Ordinance.

(a) Principle 1 – purpose and manner of collection

This provides for the lawful and fair collection of personal data and sets out the information a data user must give to a data subject when collecting personal data from that subject.

(b) Principle 2 – accuracy and duration of retention

This provides that personal data should be accurate, up-to-date and kept no longer than necessary.

## Appendix I (cont'd)

(c) Principle 3 – use of personal data

This provides that unless the data subject gives consent, personal data should only be used for the purposes for which they were collected or of a directly related purpose.

(d) Principle 4 – security of personal data

This requires appropriate security measures to be applied to personal data.

(e) Principle 5 – information to be generally available

This provides that all practicable steps should be taken to ensure that individuals can:

- (i) ascertain data users' policies and practices in relation to personal data;
- (ii) be informed of the kinds of personal data held by data users; and
- (iii) be informed of the main purposes for which personal data held by data users are or are to be used.

(f) Principle 6 – access to personal data

This provides for data subjects to have rights of access to and correction of their personal data.

A.I.5 The Ordinance 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. Any charge for providing a copy of personal data to a data subject should not be excessive. Data subjects may complain to the Commissioner about a suspected breach of the Ordinance's requirements and claim compensation for damage caused to them as a result of a contravention of the Ordinance.

**Appendix I (cont'd)****The Privacy Commissioner for Personal Data**

A.I.6 The Commissioner, who is appointed by the Chief Executive of the Hong Kong Special Administrative Region, heads the Privacy Commissioner for Personal Data Office (Office). The duties of the Commissioner include:

- (a) overseeing the administration and supervision of the Office;
- (b) formulating operational policies and procedures to implement the provisions of the Ordinance;
- (c) monitoring and supervising compliance with the provisions of the Ordinance;
- (d) exercising powers to approve and issue codes of practice providing practical guidance for compliance with the provisions of the Ordinance;
- (e) promoting awareness and understanding of, and compliance with, the provisions of the Ordinance;
- (f) examining any proposed legislation (including subsidiary legislation) that the Commissioner considers may affect the privacy of individuals in relation to personal data and report the results of the examination to the persons proposing the legislation;
- (g) carrying out inspections of personal data systems including those of Government departments and statutory corporations;
- (h) investigating, upon receipt of complaints from data subjects or on his own initiative, suspected breaches of requirements of the Ordinance;
- (i) undertaking research into, and monitoring developments in, the processing of data and computer technology that may have adverse effects on the privacy of individuals in relation to personal data; and
- (j) liaising and co-operating with persons performing similar data protection functions in any place outside Hong Kong in respect of matters of mutual interest concerning the privacy of individuals in relation to personal data.

**Appendix I (cont'd)****Exemptions**

A.I.7 The Ordinance provides specific exemptions from the requirements of the Ordinance, which include:

- (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 access to certain employment related personal data by data subjects; and
- (c) exemptions from the requirements of access to and limitation of use of personal data by data subjects as specified under the Ordinance where their application is likely to prejudice certain competing public or social interests, such as:
  - (i) security, defence and international relations;
  - (ii) prevention or detection of crime;
  - (iii) assessment or collection of any tax or duty;
  - (iv) news activities; and
  - (v) health matters.

**Offences and compensation**

A.I.8 There are a variety of offences, for example non-compliance with an enforcement notice served by the Commissioner carries a maximum penalty of HK\$50,000 and imprisonment for two years.

A.I.9 Any individual who suffers damage, including injured feeling, because of a contravention of the Ordinance by the data user concerned, is entitled to seek compensation for that damage.

Source: *Office of the Privacy Commissioner for Personal Data, Hong Kong (2008)*.

---

---

**Appendix II****The incident of the leakage of personal data held by  
the Independent Police Complaints Council on the Internet****Background**

A.II.1 On 10 March 2006, a local newspaper reported that personal data of more than 20 000 people who had made complaints to the Police held by the Independent Police Complaints Council (IPCC) had been posted on the Internet and became accessible by the Internet users. On 15 March 2006, the Commissioner initiated an investigation. After commencement of the investigation, the Commissioner received a total of 55 complaints made against IPCC.

A.II.2 In the investigation report, the Commissioner found that IPCC had contravened the requirements of data protection principle 4 (DPP4) of Schedule 1 to the Ordinance. DPP4 provides that a data user shall take all reasonably practicable steps to ensure that personal data held by it are protected against unauthorized or accidental access, processing, erasure or other use. It requires a data user to implement security safeguards and precautions in relation to the personal data in its possession, the level of which should reflect the sensitivity of the data and the seriousness of the potential harm that may result from a security breach.

A.II.3 The basis of the Commissioner's findings was that IPCC had failed to take the following actions:

- (a) steps to prevent the data from being released to the outsourced information technology contractor without due consideration of the necessity of doing so;
- (b) precautionary measures to safeguard the data that had been released to the outsourced contractor; and
- (c) practicable steps to ensure the integrity, prudence and competence of persons having access to the data, resulting in the leakage of the data on the Internet.

A.II.4 In the exercise of his power under section 50 of the Ordinance, the Commissioner issued an enforcement notice to IPCC on 18 September 2006 directing it to do the following by 16 October 2006:

- (a) devising the necessary policy and practical guidelines for the proper handling and protection of the complaint data when dealing with an outsourced contractor or agent;

**Appendix II (cont'd)**

- (b) implementing effective measures to ensure compliance by its staff with those policy and guidelines; and
- (c) reviewing the existing outsourcing contracts and endeavouring to incorporate into those contracts terms in respect of measures required to be taken by the contractors to protect the complaint data handed to them by IPCC.

A.II.5 As the Commissioner found that IPCC had complied fully with the enforcement notice, no prosecution was made.

---

---

**Appendix III****Selected incidents relating to the leakage of personal data**Incidents concerning medical institutions

A.III.1 On 25 April 2008, two incidents of the loss of USB memory sticks containing patients' data in the Tuen Mun Child Assessment Centre under the management of the Director of Health and the United Christian Hospital were reported. The number of patients involved was 700.

A.III.2 On 5 May 2008, the Chief Executive of the Hospital Authority announced that there had been nine incidents relating to the loss of electronic devices containing patients' personal data between April 2007 and April 2008 in five hospitals. Among them, eight cases had been reported to the Police, and seven cases out of these eight cases were theft-related. These data loss cases happened at Pamela Youde Nethersole Eastern Hospital (four cases), Kowloon Hospital (two cases), Queen Mary Hospital (one case), Tuen Mun Hospital (one case) and United Christian Hospital (one case). The lost electronic devices included four USB memory sticks, one palm handheld device, one MP3 player, one Central Processing Unit, one laptop computer and one digital camera. The total number of patients involved was about 6 000.

A.III.3 On 6 May 2008, the Prince of Wales Hospital revealed that a USB flash drive containing 10 000 patients' personal data was lost in early May 2008.

A.III.4 In June 2008, the Tseung Kwan O Hospital wrongly dumped 300 patients' medical reports in a landfill site.

Incidents concerning government bureaux/departments

A.III.5 In October 2006, the Leisure and Cultural Services Department wrongfully up-loaded the personal data of some guardians of the participants of the 2009 East Asian Games Slogan Competition on the Internet.

A.III.6 In December 2006, the Police Department reported a leak of personal information from the police database. The leaked data included identifying details such as the rank and mobile phone numbers of some 900 police officers, and some training materials.

A.III.7 In April 2007, personal data related to trademark registration were wrongfully disclosed through the Intellectual Property Department's website.

**Appendix III (cont'd)**

A.III.8 In July 2007, the personal particulars of 13 400 taxpayers, including their identity card numbers, residential addresses and telephone numbers, were recorded by an Inland Revenue Department's taxation officer for his future personal use.

A.III.9 In April 2008, the Civil Service Bureau revealed that the Secretariat on Civil Service Discipline reported the loss of a USB flash drive containing information on 25 civil servants and two disciplinary inquiries on alleged misconduct by two civil servants.

A.III.10 In May 2008, the Department of Immigration revealed a case of leakage of personal data. An immigration officer took, without authorization, some old classified files home to familiarize himself with working procedures. Accidentally, the files which contained watch-lists of those needing special monitoring, complaints against immigration officers and records of operational mistakes made by immigration officers were distributed on the Internet by a file-sharing programme called Foxy.

A.III.11 On 20 May 2008, the Social Welfare Department revealed that it had lost its clients' and visitors' personal data from the Kai Ping Integrated Family Service Centre in Kwun Tong in March 2008. About 10 record books containing the names of clients visited by department staff as well as client addresses and phone numbers, and visitor registration books containing recorded names and some identity card numbers of visitors to the centre were lost. On 23 May 2008, those 10 record books containing personal data lost from the department in March 2008 were found on the doorstep of the department's headquarters in Wan Chai.

A.III.12 In May 2008, documents detailing police undercover operations were found on the Internet. At least nine copies of classified documents, including investigation reports and information report forms, were discovered through a file-sharing programme called Foxy. Leaked data included some police officers' nicknames, operational procedures and victims' personal data.

A.III.13 In May 2008, the Food and Environmental Hygiene Department revealed that 170 departmental employees' work injury information was wrongly sent by an e-mail to a complainant.

A.III.14 In June 2008, the hkedcity.net, which is owned by the Government, wrongfully up-loaded the personal data of some 80 students and girl guides on its website.

**Appendix III (cont'd)**Incident concerning a bank

A.III.15 The Hongkong and Shanghai Banking Corporation (HSBC) reported that a computer server from its Kwun Tong branch, which had been undergoing renovation, was lost on 26 April 2008. The server contained personal data of 159 000 customers. The personal data included customer names, account numbers and transaction information. HSBC stated that the server did not keep PINs (personal identification numbers), passwords or user identity card numbers.

Incidents concerning tertiary educational institutions

A.III.16 In March 2007, the Hong Kong Institute of Education accidentally disclosed the personal data of about 200 students on its website.

A.III.17 In June 2007, the Hong Kong Polytechnic University made a human error which led to 1 780 students receiving other people's examination result slips via e-mail.

A.III.18 In August 2007, the City University of Hong Kong wrongly uploaded the personal data of 68 applicants of an undergraduate programme offered by the Department of Building and Construction on the Internet.

Incident concerning a computer company

A.III.19 In February 2008, sexual photographs of a Hong Kong male artiste and several female celebrities in compromising positions began appearing in Internet forums. Reportedly, the male artiste had taken his computer which contained his private photo album to a shop for repairs. The repairman downloaded his album and published its contents on the Internet.

Incident concerning a recruitment website

A.III.20 In June 2007, a recruitment website Recruit.net leaked the personal data of 40 000 online job seekers. The leaked data reportedly concerned people who had registered on the website to look for jobs between 2001 and 2006. It contained their names, addresses, phone numbers, curriculum vitae and salaries.

**Appendix III (cont'd)**

Incident concerning an insurance company

A.III.21 In March 2006, the ING Life leaked about 600 insurance policyholders' personal data, including the type and amount of coverage bought, beneficiaries' names, phone numbers, dates of birth and addresses, on the Internet.

Incident concerning a telecommunications company

A.III.22 In March 2006, a telecommunications company CSL leaked the personal records of about 500 customers on the Internet.

## **Appendix IV**

### **Some basic information about the case of Mr Shi Tao**

#### **Background**

A.IV.1 In October 2005, local newspapers reported that a mainland journalist, Mr Shi Tao, was convicted by a People Republic of China (PRC) Court of the crime of providing State secrets to foreign entities. A Hong Kong e-mail service provider, Yahoo!Hong Kong Limited (YHKL), was alleged to have disclosed Mr Shi Tao's personal data to the PRC law enforcement authorities which eventually led to Mr Shi Tao's arrest and conviction.

A.IV.2 As e-mail service providers collect and hold a massive amount of e-mail account holders' personal data, this incident aroused public concern about the protection of e-mail subscribers' personal data privacy, in particular where disclosure is made in compliance with a lawful order issued by a foreign authority under foreign law for purpose of investigation of a foreign crime.

A.IV.3 On 21 October 2005, the Commissioner took the initiative to probe into the matter to determine whether there had been a breach of the Ordinance. Subsequently, the Commissioner received a complaint lodged by an authorized representative of Mr Shi Tao alleging that YHKL had disclosed Mr Shi Tao's personal data to the PRC authorities without his consent. The Commissioner decided to carry out an investigation pursuant to section 38 of the Ordinance on 9 May 2006.

#### **Findings of the investigation**

A.IV.4 On 14 March 2007, the Commissioner published a report on the result of an investigation of the alleged disclosure by an e-mail service provider in Hong Kong of its account subscriber's personal data. He concluded that YHKL had not contravened the Ordinance because an Internet Protocol address per se did not meet the definition of "personal data". In addition, there was insufficient evidence to prove that Mr Shi Tao's personal data were disclosed by YHKL to the PRC authorities. Hence there had been no contravention of the requirements of the Ordinance by YHKL. No enforcement notice was issued in consequence of the investigation.

---

---

## References

1. Berthold, M. & Wacks, R. (1997) *Data Privacy Law in Hong Kong*. 1<sup>st</sup> ed. China, FT Law & Tax Asia Pacific.
2. Berthold, M. & Wacks, R. (2003) *Hong Kong Data Privacy Law: Territorial Regulation in a Borderless World*. 2<sup>nd</sup> ed. Hong Kong, Sweet & Maxwell Asia.
3. Commerce, Industry and Technology Bureau. (2006) *Information Security*. Paper submitted to the Panel on Information Technology and Broadcasting of the Legislative Council for information on 17 March 2006. LC Paper No. CB(1)1097/05-06(01). Available from: <http://www.legco.gov.hk/yr05-06/english/panels/itb/papers/itb0317cb1-1097-1e.pdf> [Accessed April 2008].
4. Constitutional Affairs Bureau. (2001) *Applicability of the HKSAR laws to the offices set up by the Central Peoples's Government in the HKSAR*. Paper submitted to the Panel on Administration of Justice and Legal Services of the Legislative Council. LC Paper No. CB(2)1907/00-01(09). Available from <http://www.legco.gov.hk/yr00-01/english/panels/ajls/papers/b1907e09.pdf> [Accessed April 2008].
5. Constitutional and Mainland Affairs Bureau. (2007) *Press Releases: LCQ9 – Protection of personal data*. Available from: [http://www.cmab.gov.hk/en/press/press\\_1560.htm](http://www.cmab.gov.hk/en/press/press_1560.htm) [Accessed March 2008].
6. *Data Protection Act 1998, Chapter 29*. Available from: [http://www.opsi.gov.uk/Acts/Acts1998/ukpga\\_19980029\\_en\\_1](http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1) [Accessed May 2008].
7. Hong Kong Information Services Department. (2007) *Privacy law review urged*. Available from: <http://www.news.gov.hk/en/category/healthandcommunity/070314/html/070314en05006.htm> [Accessed April 2008].
8. *Hong Kong's Personal Data (Privacy) Ordinance 1995*. Available from: <http://www.austlii.edu.au/au/journals/PLPR/1995/105.html> [Accessed April 2008].
9. Lau, S. (2001) *Personal Data (Privacy) Ordinance and The Office of the Privacy Commissioner for Personal Data Hong Kong SAR*. Available from: [http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/\(03995EABC73F94816C2AF4AA2645824B\)~Laupaper.pdf/\\$file/Laupaper.pdf](http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~Laupaper.pdf/$file/Laupaper.pdf) [Accessed April 2008].

- 
10. Legislative Council Secretariat. (1995) *Report of the Bills Committee to study Personal Data (Privacy) Bill*. Paper submitted to the House Committee of the Legislative Council for information on 14 July 1995. LC Paper No. HB1185/94-95.
  11. Legislative Council Secretariat. (2008a) *Council Meeting (Agenda) 21 May*. Available from: <http://www.legco.gov.hk/yr07-08/english/counmtg/agenda/cmtg0521.htm> [Accessed May 2008].
  12. Legislative Council Secretariat. (2008b) *Council Meeting (Agenda) 28 May*. Available from: <http://www.legco.gov.hk/yr07-08/english/counmtg/agenda/cmtg0528.htm> [Accessed May 2008].
  13. *Minutes of Meeting of the Panel on Home Affairs of the Legislative Council*. (2007) 11 October. LC Paper No. CB(2)246/07-08.
  14. Office of the Privacy Commissioner for Personal Data, Hong Kong. (2006) *Data Protection Principles in the Personal Data (Privacy) Ordinance: from the Privacy Commissioner's perspective*. Hong Kong.
  15. *Office of the Privacy Commissioner for Personal Data, Hong Kong*. (2008) Available from: <http://www.pcpd.org.hk/engindex.html> [Accessed April 2008].
  16. Office of the Privacy Commissioner for Personal Data, Hong Kong. (various years) *Annual Report 1996-2007*.
  17. *Personal Data (Privacy) Bill*. (1995)
  18. *Personal Data (Privacy) Ordinance*. Available from: <http://www.pcpd.org.hk/english/ordinance/down.html> [Accessed April 2008].
  19. The Government of the Hong Kong Special Administration Region. (2006) *Press Releases: LCQ17 – IP addresses as personal data*. Available from: <http://www.info.gov.hk/gia/general/200605/03/P200605030211.htm> [Accessed April 2008].
  20. The Law Reform Commission of Hong Kong. (2004) *Civil liability for invasion of privacy*. Hong Kong, Government Logistics Department.
  21. Wisers Information Limited. (2008) *LegCo News Clipping Services*. From 4 December 2004 to 25 June 2008.