Unauthorised Disclosure of Information Relating to Telecommunications Service Subscribers: Paper for Legislative Council Panel on Security

Introduction

This note is prepared in response to a request from the Clerk to Legislative Council's Security Panel in a letter dated 3 August 1998 for information on:

- the trend in abuse and unauthorised disclosure of personal data relating to subscribers of telecommunications service; and

- joint efforts to be taken by the Privacy Commissioner's Office ("PCO") and the ICAC to safeguard against unauthorised disclosure of personal information in the public and private sectors.

A short note on the application of the requirements of the Personal Data (Privacy) Ordinance ("the Ordinance") to this issue is at Annex I for reference.

Complaint Case Trends

2. Between 20 December 1996, the date of the general commencement of the Ordinance, and 31 July 1998, the PCO received 465 complaints. Of these, 33 complaints were against organisations in the telecommunications industry, 12 of which related to claims of unauthorised disclosure of personal data. Following detailed investigation no contravention of the requirements of the Ordinance was established in any of the 12 complaint cases concerned. Where deficiencies in the relevant practices of the parties were identified in the course of the investigations, they were required to make appropriate improvements. A summary of some of the complaints cases involving the telecommunications sector is attached at Annex II for reference

Action taken by the PCO

3. In March 1998, following a number of high profile reported cases of unauthorised disclosure of customer information, the Privacy Commissioner wrote to representative bodies in the financial and insurance sectors, individual companies in the telecommunications sector and public utility companies drawing attention to the need to ensure security in relation to personal data. The letter drew particular attention to the need to take measures to protect against security breaches by employees who have the authority to access personal data held by the organisation concerned (copy of letter attached at Annex III for reference). The same message was conveyed to the public sector in a briefing for Heads of Departments by the Privacy Commissioner on 26 March, 1998.

4. The PCO has met with the ICAC to discuss the scope for mutual assistance in preventing the unauthorised disclosure of client information. We understand that the ICAC is considering guidelines for the telecommunications industry and will consult the PCO on the draft guidelines.

5. Lastly, in May this year the PCO wrote to the Telecommunication Association of Hong Kong enclosing the case notes at Annex II. The Association was invited to circulate the notes to its members in order that they could be informed of the sort of complaint cases received regarding the industry and the PCO's views on them.

Office of the Privacy Commissioner for Personal Data
August 1998

Annex I

Unauthorised Disclosure of Personal Data

As a general matter, the use of personal data is subject to the requirements of data protection principle ("DPP") 3 in Schedule 1 to the Personal Data (Privacy) Ordinance. DPP 3 provides that the use of personal data, which includes the disclosure of personal data or information inferred from the data, shall be limited to the purposes for which the data were collected or directly related purposes, unless the subject of the data consents otherwise expressly and voluntarily. In addition, DPP4 provides that all reasonably practicable steps shall be taken to ensure that personal data are protected against, inter alia, unauthorised disclosure or other use.

2. Where a staff member of a public or private sector organisation uses or discloses personal data of a client without proper authority, he or she may be in breach of DPP 3. In addition, if the organsiation has failed to take all reasonably practicable steps to prevent this from happening, then it may be in breach of DPP4. A breach of a DPP is not itself an offence. (Hence, if the act concerned is suspected to be an offence under a different ordinance, it would be appropriate for that to be the first subject of any investigation.) However, the Privacy Commissioner has the power to issue an enforcement notice if he is of the opinion following an investigation by him that a contravention of a DPP has occurred and is likely to be repeated or continue (section 50 of the Ordinance refers). In addition, a party who suffers any damage, including injury to feelings, as a result of the breach of a DPP may recover against the party in breach for such damage (section 66 of the Ordinance refers). Moreover, an employer is liable for an act of an employee that is a breach of a DPP unless the employer has taken all reasonably practicable steps to prevent the act (section 65 of the Ordinance refers).

Office of the Privacy Commissioner for Personal Data
August 1998

Complaints against Telecommunication service organisations

During the period from the commencement of the Personal Data (Privacy) Ordinance on 20 December 1996 to 31 July 1998, the Privacy Commissioner's Office ("PCO") received 33 complaint cases in relation to telecommunication service organisations. Of these 33 cases, 12 cases related to alleged unauthorised disclosure of personal data of the complainants contrary to the requirements of data protection principle 3 ("DPP3") which provides that personal data shall not, without the prescribed consent of an individual, be used for any purpose other than the purpose for which the data were to be used at the time of the collection of the data or a directly related purpose. The following summaries provide a brief account of some of the cases investigated by the PCO.

Cases related to unauthorised disclosure subscribers' personal data

- The complainant was a customer of a telephone company and its subsidiary mobile phone company. In registering for the respective services, the complainant used two different addresses. He complained that the telephone company used his address registered under the subsidiary company for the purpose of collecting his outstanding residential telephone line charge. Upon investigation, the PCO found no evidence showing that the telephone company obtained the address by an internal transfer from its subsidiary. The address used by the company's appointed debt collection agency was obtained from the envelope of a returned demand letter that had originally been sent to the complainant's registered address with the telephone company. The person who had written the address on the envelope of the returned letter was unknown. As it could not be established who wrote the address, the PCO took the view that no contravention of DPP3 could be ascertained.

- The complainant applied for an account with a mobile phone service company. She complained that the company had, without her consent, passed her personal data to an IDD service company to open an account for its IDD service in her name. In the course of investigation by the PCO, it was found that it was a staff member of the company, acting in contravention of the company's internal policies, who had used the complainant's personal data and forged her signature to open an IDD account in her name. The PCO was satisfied that the company had taken all reasonably practicable steps to prevent its staff from committing the act complained of and in view of section 65(3) of the Ordinance, the company would not be liable for the act done by the staff. Section 65(3) of the Ordinance provides that it shall be a defence for a person in respect of any act done by his employees to prove that he has taken practicable steps to prevent the employee from doing that act.

- The complainant had applied for ex-directory service with a telephone company. However, the complainant repeatedly received nuisance calls from a third party and complained to the PCO about suspected disclosure of his telephone number by the telephone company. In the course of the inquiry with the company, the PCO did not find evidence to substantiate a breach of the Ordinance but cautioned that the company should undertake regular reviews of its policy and procedures and implement audit measures to ensure its staff complied with its policy.

- The complainant was a subscriber of a paging company. She complained that the paging company disclosed her pager messages to her friend who had knowledge of her pager account number. Upon inquiry by the PCO, it was found that the paging company had implemented procedures whereby retrieval to subscribers' messages would only be disclosed upon the provision and verification of account number and access password of the account holder. An examination of the computer log held by the paging company did not reveal any unauthorised retrieval of the complainant's messages.

- Six cases in which the complainants were in default of service payment due to the mobile service companies. They complained that the companies disclosed their personal data to debt collection agencies for pursuing the overdue payments. The PCO takes the view that when data users collect personal data in relation to a provision of service, disclosure of the data to a debt collector for the purpose of recovery of any sum owed by the data subject under that service provision is a purpose directly related to the original purpose of collection. However, any data which were not relevant to the purpose of recovering the debt or would otherwise be excessive, should not be disclosed.

Cases related to unauthorised disclosure of employees' data

- The complainant was dismissed from service as a paging operator by her employer. In the course of searching for a new job, she found that her name and the reasons of her termination from service were circulated amongst other paging companies. She complained that her previous employer disclosed her personal data without her consent. The PCO had no jurisdiction to handle the case as the incident occurred prior to the Ordinance came into force. However, the PCO takes the view that the practice of "blacklisting" a candidate by disclosing personal data of an exemployee without consent to other parties might amount to a breach of DPP3 unless there are applicable exemptions provided by the Ordinance.

Annex III

Our Ref: PCO/7/14

March 13, 1998 (by post)

Dear

Within the last few weeks, there have been a number of incidents reported in the press relating to the unauthorised disclosure of personal data to third parties by staff of organisations with large customer databases. Such an incident might lead to, and so far in at least one case has led to, criminal prosecution and conviction of the staff member concerned with attendant negative publicity for the organisation concerned. They have also caused concern among the community in Hong Kong as some of these organisations do hold personal data of hundreds of thousands of Hong Kong citizens.

I am aware that your member organisations have privacy policies and practices with regard to personal data and have implemented security measures to protect unauthorised access, use and disclosure of such personal data. However, the reported incidents indicate that the disclosure of personal data was effected by personnel who were authorised to access personal data as part of their job functions. While such improper acts by personnel who have authority to access personal data pose difficult management problems, I believe that measurcs can be taken to minimise such acts. Some examples of these measures are given below.

- **All** personal data held should be treated as confidential information and accorded the stringent level of protection commensurate with that grading. While some personal data are generally regarded as being more sensitive than others, e.g. financial-related personal data, the reported incidents highlight the fact that even the misuse of data that are not generally regarded as highly sensitive, e.g. a telephone number, could be connected to serious criminal activities;

- Detailed audit trails of database accesses by all persons, including authorised personnel, should be maintained and subjected to regular supervisory reviews which could uncover anomalous behaviour;

- Checks and balances should be implemented with respect to access procedures with the involvement of more than one person to carry out access to company database

Such measures, together with appropriate training for relevant staff and constant reminders of their responsibilities to respect the personal data of customers and ensure security with respect to such data, could serve both detection and deterrent purposes.

I wish to emphasise that in no way does this letter imply any shortcoming in your member organisations with respect to the protection of personal data or their security measures. My intention is simply to further heighten the awareness of the possible serious consequences of the misuse of personal data held by your member organisations, particularly given the large volume of such data held by the banking industry. I like to suggest to your member organisations to consider instituting a senior management review of their current data protection measures and procedures to reaffirm their effectiveness and, if appropriate, to seek further improvements.

I welcome your views, and that of your member organisations, on this matter in our mutual wish to ensure personal data protection in the interests of the community. I look forward to hearing from you.

Yours sincerely

Stephen Lau
Privacy Commissioner for Personal Data

LETTERHEAD OF GOVERNMENT SECRETARIAT
LOWER ALBERT ROAD
HONG KONG

本函檔號 OUR REF.: (23) in SBCR 1/7/1476/92(98) Pt.9
來函檔號 YOUR REF.:

Our Tel.:2810 2641 28 August 1998
Our Fax:2523 4171

Miss Betty Ma,
Senior Assistant Secretary (2)1,
Legislative Council,
Legislative Council Building,
8 Jackson Road, Central,
Hong Kong.

Dear Miss Ma,

Unauthorised access into the Airport Restricted Area

As per your request, we append below the number of cases of unauthorised access into the Airport Restricted Area in the recent weeks of airport operation, in addition to the information we gave vide our letter of 25 July for Members' information:

	A. With invalid permit	B. Using other person's permit	C. Without wearing any permit	Total
Number in the 4th week	3	0	4	7
Number in the 5th week	3	0	2	5
Number in the 6th week	3	1	0	4
Number in the 7th week	1	2	0	3

Yours sincerely,

(Donald Ng)
for Secretary for Security