

**Report Published under Section 48(2) of the  
Personal Data (Privacy) Ordinance (Cap. 486)**

根據《個人資料（私隱）條例》（第 486 章）第 48（2）條  
發表的報告

**Report Number: R06-2599**      報告編號：R06-2599

**Date issued: 26 October 2006**      發表日期：2006 年 10 月 26 日



香港個人資料私隱專員公署  
Office of the Privacy Commissioner  
for Personal Data, Hong Kong

**Must Take Security Measures to Protect Personal Data  
when Engaging Outsourced Contractor**

**Case number: 200602599**

This report in respect of an investigation carried out by me pursuant to section 38 of the Personal Data (Privacy) Ordinance, Cap 486 (the “Ordinance”) against the Independent Police Complaints Council is published in the exercise of the power conferred on me by Part VII of the Ordinance. Section 48(2) of the Ordinance provides that “*the Commissioner may, after completing an investigation and if he is of the opinion that it is in the public interest to do so, publish a report –*

(a) *setting out –*

(i) *the result of the investigation;*

(ii) *any recommendations arising from the investigation that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the class of data users to which the relevant data user belongs; and*

(iii) *such other comments arising from the investigation as he thinks fit to make; and*

(b) *in such manner as he thinks fit.”*

**Roderick B. WOO**  
**Privacy Commissioner for Personal Data**

## Table of Contents

<b>CHAPTER ONE</b> .....	<b>1</b>
Introduction .....	1
Introduction .....	1
The Incident .....	2
The Parties Involved .....	3
<b>CHAPTER TWO</b> .....	<b>4</b>
Methodology .....	4
<b>CHAPTER THREE</b> .....	<b>6</b>
The System of Managing Complaints against the Police .....	6
IPCC .....	6
Secretariat of IPCC .....	6
CAPO .....	8
Processing of Complaints against the Police .....	9
<b>CHAPTER FOUR</b> .....	<b>12</b>
The IPCC Information Technology System .....	12
Complaint Statistics .....	12
Development of the Computer Statistical System .....	13
First Enhancement Programme .....	14
Matching Programme .....	14
Second Enhancement Programme .....	15
Maintenance Contracts .....	15
<b>CHAPTER FIVE</b> .....	<b>16</b>
Security and Privacy Policies .....	16
Security Policies .....	16
Privacy Policy .....	17
<b>CHAPTER SIX</b> .....	<b>18</b>
Events Leading to the Leakage on the Internet .....	18
Introduction .....	18
Transfer of Data from IPCC to EDPS from May 2000 to May 2003 ....	18
Transfer of Data from IPCC to EDPS from May 2003 to March 2006 .	19
Discrepancies between the Versions from IPCC and EDPS.....	20

Leakage of the Complainants’ Personal Data on the Internet .....	22
Other Witnesses.....	24
<b>CHAPTER SEVEN.....</b>	<b>25</b>
The Commissioner’s Findings.....	25
The Commissioner’s Findings against IPCC.....	25
Comments on the Parts Played by Other Parties in the Incident .....	28
<i>Comments relating to CAPO.....</i>	28
<i>Comments relating to EDPS .....</i>	29
<i>Comments relating to Mr. Y .....</i>	30
<i>Comments relating to Ms. X and her then Supervisor .....</i>	31
<i>Comments relating to the Webmaster .....</i>	32
<b>CHAPTER EIGHT.....</b>	<b>34</b>
Actions Taken by IPCC after the Leakage and Recommendations by the Commissioner .....	34
Actions Taken by IPCC after the Leakage .....	34
Enforcement Notice.....	35
Recommendations Arising from the Investigation.....	36
<i>Measures to be Taken when Engaging Outsourced Contractor or         Agent .....</i>	36
<i>Recommended Practice for IT Practitioners .....</i>	38
<i>Guidance to Government Officers.....</i>	39
 <b><u>ANNEXES</u></b>	
<b>Annex A – IPCC Report on Leakage of Personal Data (8 April 2006)</b>	
<b>Annex B – IPCC Internal Circular No. 37/98 titled “Handling of Classified Documents”</b>	

# CHAPTER ONE

## Introduction

### Introduction

1.1.1 This report pertains to the investigation carried out by the Privacy Commissioner for Personal Data (the “Commissioner”) pursuant to section 38 of the Personal Data (Privacy) Ordinance, Chapter 486 (the “Ordinance”) in respect of the leakage on the Internet of personal data relating to complaints made against the Police by the public (the “Incident”).

1.1.2 Subsequent to the Commissioner’s decision to commence investigation against the data user, a total of 55 complainants filed complaints with the Commissioner’s Office. The investigation therefore is directed at the Independent Police Complaints Council (“IPCC”) which is the subject of the complaints.

1.1.3 Of relevance to this case is the requirement stipulated by data protection principle 4 (“DPP4”) in Schedule 1 to the Ordinance, which provides that:

*“Principle 4 – security of personal data*

*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 Incident**

1.2.1 On 10 March 2006, a news report captioned “*20,000 put at risk by blunder on identities*” was published in a local newspaper. It was stated in the report that a database apparently from IPCC containing complaint information of the Complaints Against Police Office (“CAPO”), including names, addresses and identity card numbers of the complainants, was found accessible by the public via a website [www.china2easy.com](http://www.china2easy.com) (the “Website”). The data were removed from the Website on the same day after the newspaper contacted the registered operator of the Website.

1.2.2 The Commissioner decided to take immediate action before any formal complaint was received. On 10 March 2006, the same day on which the news report was published the Commissioner’s Office promptly made a written inquiry to IPCC. On 11 March 2006, the Commissioner contacted the Chairman of IPCC and obtained some preliminary facts of the Incident. Arrangement was also made to meet some senior personnel of IPCC. On 13 March 2006, the Commissioner interviewed the Chairman and a Vice-chairman of IPCC. On the same day, he also led his senior officers to meet the senior staff of IPCC. On 15 March 2006, a formal investigation was initiated by the Commissioner under section 38(b) of the Ordinance.

1.2.3 IPCC released its report on the Incident on 8 April 2006. A copy of the IPCC report is at Annex A. Meanwhile, the Commissioner received a number of complaints from individuals affected by the Incident. After verifying the identities of the complainants and satisfying that their personal data were leaked on the Internet, investigations of the complaints were carried out under section 38(a) of the Ordinance.

1.2.4 The table below shows the number of complaints received by the Commissioner's Office up to the writing of this report:

Period	Number of complaints received
13 Mar 2006 - 19 Mar 2006	9
20 Mar 2006 - 26 Mar 2006	3
27 Mar 2006 - 02 Apr 2006	7
03 Apr 2006 - 09 Apr 2006	2
10 Apr 2006 - 16 Apr 2006	6
17 Apr 2006 - 23 Apr 2006	2
24 Apr 2006 - 30 Apr 2006	2
01 May 2006 - 07 May 2006	2
08 May 2006 - 14 May 2006	6
15 May 2006 - 21 May 2006	6
22 May 2006 - 28 May 2006	5
29 May 2006 - 18 Sep 2006	5
TOTAL :	55

### **The Parties Involved**

1.3.1 The party against whom complaints were made to have contravened the provisions of the Ordinance is IPCC.

1.3.2 In the course of the investigation, the Commissioner identified other relevant parties involved. Although they were not the party against whom complaints were made, the Commissioner considered it appropriate to comment on their respective roles and conduct in relation to the personal data concerned.

1.3.3 These parties include:

- (i) CAPO,
- (ii) EDPS Systems Ltd. ("EDPS"), the IPCC information technology ("IT") contractor,
- (iii) Mr. Y, EDPS's sub-contractor,
- (iv) Ms. X, an officer of IPCC,
- (v) the then supervisor of Ms. X (the "then Supervisor"), and
- (vi) the webmaster in charge of the Website (the "Webmaster").

## CHAPTER TWO

### Methodology

2.1 The investigation was carried out by way of visits to the IPCC office, visits to CAPO, interviews of the personnel concerned, examination of documentary records held by the parties involved, examination of written representations from the parties involved and interviews of relevant persons by way of summons by the Commissioner under section 44 of the Ordinance.

2.2 Officers of the Commissioner's Office visited the IPCC office on 13 March 2006 and 24 April 2006. In response to the inquiries of the Commissioner's Office, IPCC submitted written representations on 13 March 2006, 14 March 2006, 8 April 2006, 27 April 2006, 29 April 2006, 2 May 2006, 11 May 2006 and 20 May 2006. The officers of the Commissioner's Office also visited CAPO on 24 April 2006 and obtained written representations from it on 8 May 2006 and 11 May 2006. At the same time, EDPS provided written representations to the Commissioner's Office on 22 March 2006, 4 April 2006, 11 April 2006 and 16 May 2006.

2.3 In addition, the following persons were also seen, interviewed or examined by way of summons by the Commissioner and/or his officers:

- (i) Chairman of IPCC,
- (ii) Vice-chairman of IPCC,
- (iii) Secretary of IPCC,
- (iv) Deputy Secretary of IPCC,
- (v) the then Supervisor,
- (vi) Ms. X,
- (vii) two Office Assistants of IPCC,
- (viii) President of EDPS,
- (ix) General Manager of EDPS,
- (x) Mr. Y,
- (xi) Mr. Y's business partner ("Mr. Y's Partner"),
- (xii) the Webmaster,
- (xiii) Former Statistics Officer of CAPO, and



- (xiv) Information Technology Officer of the Police Information Systems Wing (the “Police Programmer”).

## **CHAPTER THREE**

### **The System of Managing Complaints against the Police**

#### **IPCC**

3.1.1 IPCC has its origin in the UMELCO Police Group which evolved into the Police Complaints Committee (PCC), a non-statutory but independent body commissioned by the then Governor in 1986. The PCC was renamed as Independent Police Complaints Council (IPCC) on 30 December 1994. IPCC presently comprises a Chairman, three Vice-chairmen and fourteen other Members appointed by the Chief Executive.

3.1.2 The main function of IPCC is to monitor and review the investigations conducted by CAPO in respect of public complaints against the Police. Its terms of reference are:

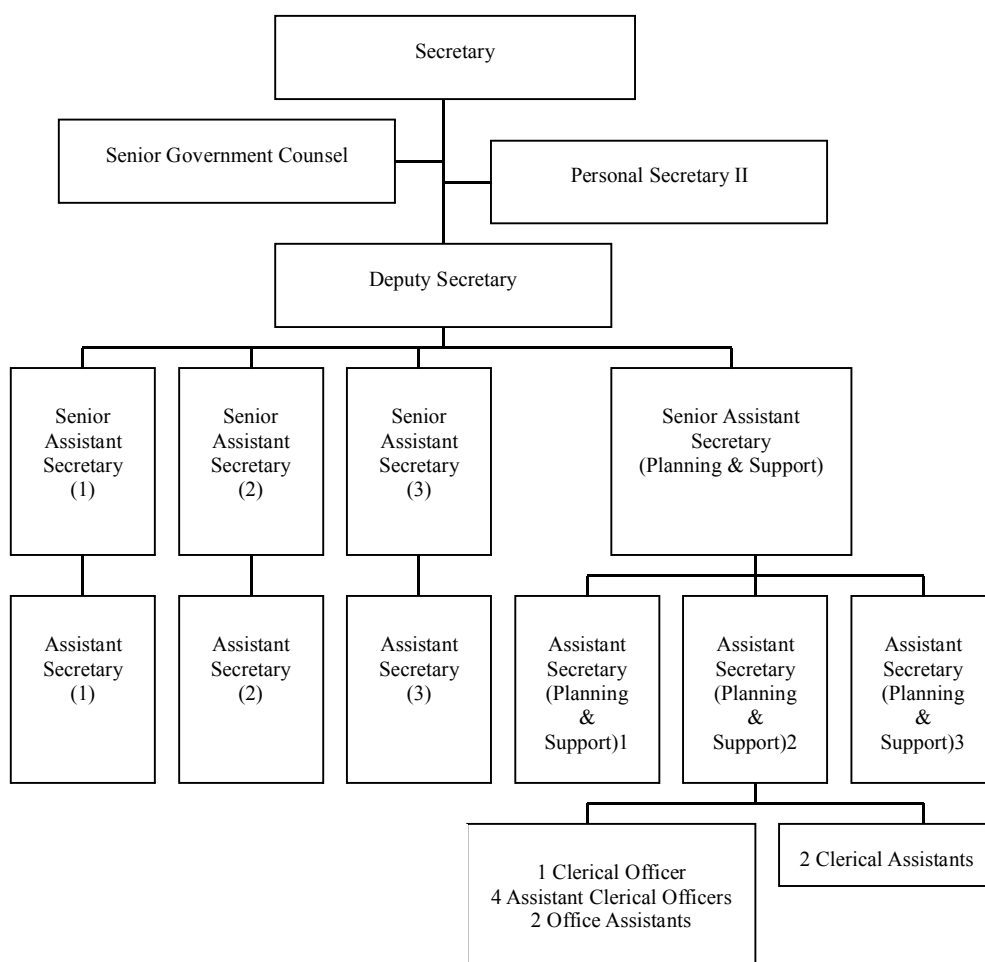
- (i) to monitor and, where it considers appropriate, to review the handling by the Police of complaints by the public;
- (ii) to keep under review statistics of the types of conduct by police officers which lead to complaints by members of the public;
- (iii) to identify any faults in Police procedures which lead or might lead to complaints; and
- (iv) where and when it considers appropriate, to make recommendations to the Commissioner of Police or, if necessary, to the Chief Executive.

#### **Secretariat of IPCC**

3.2.1 IPCC is supported by a full-time Secretariat (the “IPCC Secretariat”) which is formed by civil servants, headed by an Administrative Officer Staff Grade C (as Secretary) with 21 general grade staff and a Senior Government Counsel serving as legal adviser to IPCC. The major function of the IPCC Secretariat is to examine all complaint investigation reports submitted by CAPO in detail to ensure that each and

every case is investigated in a thorough and impartial manner before recommending them to IPCC Members for endorsement. Under the supervision of the Secretary and Deputy Secretary (a Chief Executive Officer), three teams, each comprising one Senior Assistant Secretary (SAS) and one Assistant Secretary (AS), pitched at Senior Executive Officer and Executive Officer I levels respectively, are responsible exclusively for vetting complaint investigations. The fourth team, Planning and Support, comprising one SAS and 12 executive, clerical and secretarial staff, is responsible for general administration, research, publicity and other support services as well as servicing the Serious Complaints Committee of IPCC.

3.2.2 The organizational structure of the IPCC Secretariat is as follows:

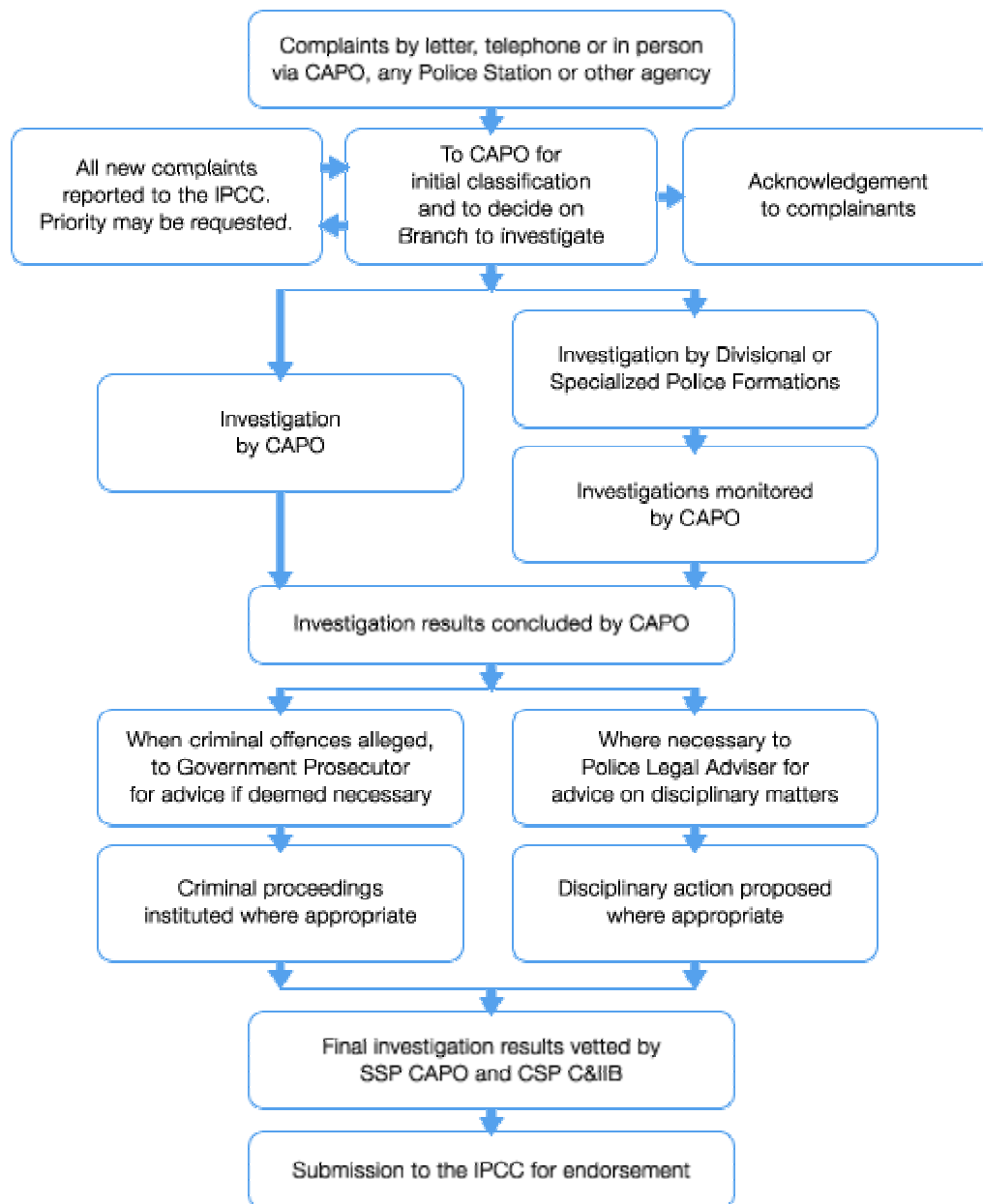


3.2.3 IPCC Members may give directives or orders to the IPCC Secretariat in respect of matters related to the carrying out of their functions and duties. The IPCC Secretariat will carry out the directives or orders of IPCC Members provided that such directives or orders are not contrary to rules or regulations governing civil servants. IPCC Members however have no authority in deciding the staffing matters of the IPCC Secretariat, including termination of employment. Save for matters of importance or at the request of IPCC Members, the IPCC Secretariat does not report its operational matters to IPCC Members.

## **CAPO**

3.3.1 CAPO belongs to the Complaints and Internal Investigation Branch (C&IIB) of the Police and is accountable to the Commissioner of Police for ensuring that all complaints of misconduct or allegations of crime made against a police officer or civilian member attached to the Police are fully and impartially investigated. All complaints, irrespective of origin, are referred to CAPO for investigation. At the conclusion of an investigation into a complaint, CAPO will compile a report detailing the investigation and findings and submit it to IPCC for endorsement. All complaints are monitored by IPCC to ensure that they have been thoroughly and impartially investigated.

3.3.2 The following flow-chart illustrates the process by which complaints are examined and investigated by CAPO. At the conclusion of an investigation, CAPO classifies a complaint according to the result and prepares a report to IPCC for review and endorsement.



**Notes**

SSP - Senior Superintendent

CSP - Chief Superintendent

**Processing of Complaints against the Police**

3.4.1 The CAPO submits to IPCC all investigation reports together with the related case or crime investigation files. These are scrutinized in detail by the Executive Officers of the IPCC Secretariat who will seek legal advice from the in-house Senior Government Counsel where necessary.

3.4.2 All CAPO reports, including the draft replies to complainants, are discussed in detail at the weekly IPCC Secretariat case conferences chaired by the Secretary.

3.4.3 After a case conference, the IPCC Secretariat raises written comments and queries, if any, with CAPO. Where appropriate, the IPCC Secretariat also draws CAPO's attention to inadequacies in existing Police policies, procedures or practices and proposes remedial measures.

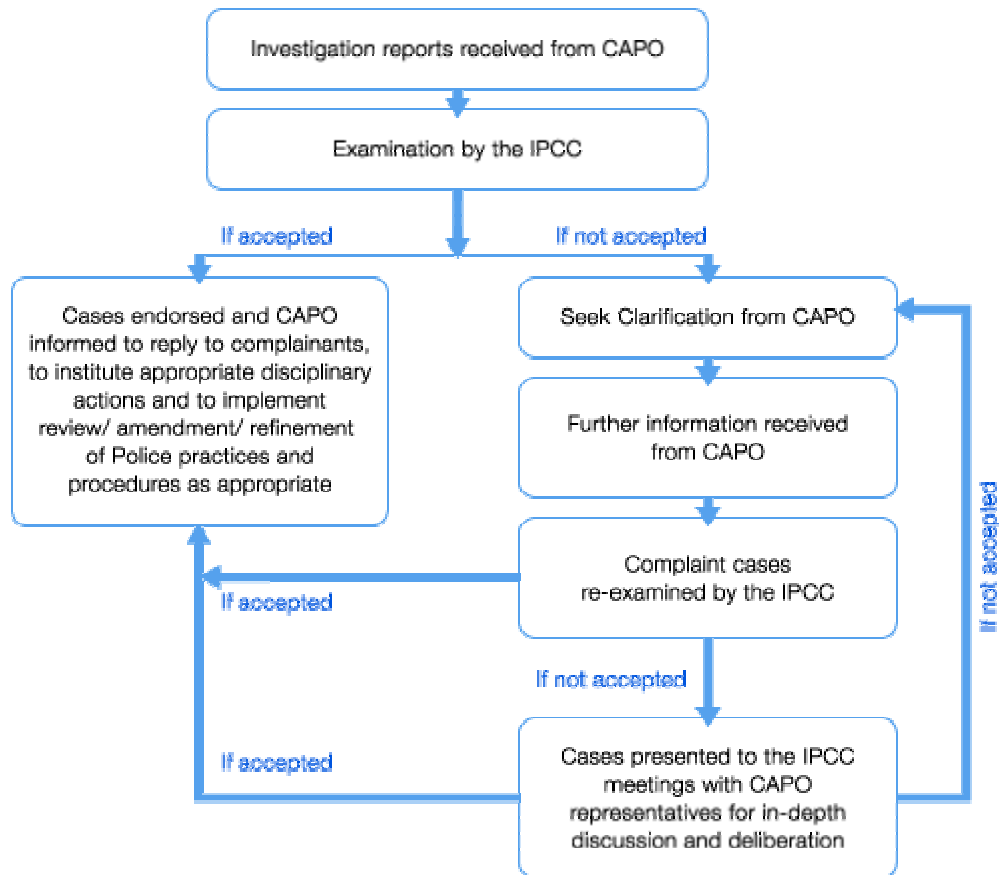
3.4.4 The replies received from CAPO are carefully reviewed by the IPCC Secretariat before preparing its own covering reports for consideration by IPCC Members. Vetted cases are submitted to IPCC Members in batches every week.

3.4.5 IPCC Members are divided into three sub-groups to share the workload. Each sub-group comprises a Vice-chairman and five Members. Each case is studied by the respective Vice-chairman and Members. The Chairman of IPCC examines all serious cases and any other cases submitted to him by the Secretary and/or any Vice-chairman or Member.

3.4.6 Sometimes, in very serious and complicated cases, the process may involve the setting up of special review panels, the interviewing of witnesses by IPCC Members and the seeking of medical and/or legal advice. If necessary, CAPO would be asked to re-investigate the case.

3.4.7 The majority of the cases are cleared by circulation of papers. However, complicated cases which involve policy implications or which cannot be resolved by correspondence between the IPCC Secretariat and CAPO are discussed at the Joint IPCC/CAPO Meetings which are chaired by the Chairman of IPCC.

3.4.8 The monitoring of CAPO's completed investigations on complaints against the Police by IPCC is illustrated as follows:



## CHAPTER FOUR

### The IPCC Information Technology System

#### Complaint Statistics

4.1.1 In order to keep under review statistics of the types of police conduct which lead or may lead to complaints by members of the public, IPCC has to maintain complaint statistics both for annual review purpose and to facilitate in-house researches to be conducted on matters relating to complaints against the Police.

4.1.2 Procedurally, complaint statistics are captured by IPCC as follows. After the complaint cases are endorsed by IPCC, case officers of IPCC would give a code to each case according to the information contained in the CAPO report files. Coding parameters include the nature of the allegation, the classification of the allegation, the circumstances of the incident, the particulars of the complainants and the persons being complained against. The coding process is necessary for the effective formulation of statistics required for analysis of the complaint data. After coding, IPCC's staff would then input the data into IPCC's computer statistical system.

4.1.3 CAPO had its own computer system called Complaints Index and Statistics System ("CISS") to manage statistics of the complaints. Although CAPO and IPCC were using the same coding table, the statistical result might sometimes be different because CAPO and IPCC carried out their coding process independently and officers of IPCC and CAPO might enter different codes in handling the same case. It was therefore necessary for CAPO and IPCC to check with one another discrepancies in the complaint data before adopting them for internal use (including in-house researches) or releasing to the public.

4.1.4 While separate statistical systems were maintained by IPCC and CAPO, IPCC had raised, during a joint meeting with CAPO in 2000, the feasibility of establishing a computer terminal in IPCC with direct linkage to CAPO's CISS. It was subsequently resolved that no direct computer



linkage would be made between IPCC and CAPO, but CAPO would provide to IPCC on a regular basis computer discs containing extracts of CISS information for the preceding 5 years.

4.1.5 Under the arrangement, CAPO would forward statistical data on complaints against the Police (with details of individual cases captured) by a computer disc to IPCC on a regular basis for verification purpose. Reports on mismatched codings would be prepared electronically. IPCC would re-examine the mismatched information and make necessary reconciliation with CAPO. The reconciled data would then be incorporated into IPCC's computer statistical system.

### **Development of the Computer Statistical System**

4.2.1 In 1998, IPCC used a computerized statistical system to manage the data and information of all the complaint cases. To manage the data in a better and more efficient way, IPCC intended to develop a new system.

4.2.2 The new system was expected to operate in a stand-alone personal computer starting from 1 January 1999 and should:

- (i) allow the creation, storage and updating of complaint records with the use of standard codes;
- (ii) allow the addition, deletion and change of the standard codes;
- (iii) allow searching/editing/sorting and statistical enquiry of complaint case records;
- (iv) allow the printing of statistical reports;
- (v) have security measures such as login password;
- (vi) be capable of further enhancement;
- (vii) be compliant with the Year 2000 system requirement; and
- (viii) be user-friendly.

4.2.3 The selected contractor for the development of the computer statistical system was expected to:

- (i) provide the necessary programming services;

- (ii) install and test the system;
- (iii) customize the computing environment for the successful operation of the system;
- (iv) provide sufficient training for the users;
- (v) provide IPCC with a user manual of the system;
- (vi) advise the necessary hardware and software platforms;
- (vii) convert and import old data from the existing database (FoxBase+ database format) into the new database;
- (viii) provide a warranty period of about six months; and
- (ix) provide maintenance services at an agreed fee, if required.

4.2.4 IPCC had issued invitations for quotations to six contractors and finally chose EDPS to provide the services. IPCC formally entered into a contract with EDPS on 24 December 1998.

4.2.5 Under the terms of the contract, EDPS agreed to provide data conversion programmes to IPCC to convert as much data as possible from the old system to the new system. EDPS would also prepare and deliver to IPCC a user manual as a reference guide. Finally, EDPS would provide maintenance services after the application software had been successfully installed and accepted by IPCC.

### **First Enhancement Programme**

4.3 Since August 1999, IPCC had further engaged EDPS to carry out enhancements of the computer statistical system. In 1999, enhancement was carried out to import special printing and search functions to the system. In 2000, more data fields and printing functions were added.

### **Matching Programme**

4.4 Around April 2001, it was found that there were minor terminology and classification grouping differences in the respective computer systems used by IPCC and CAPO for keeping complaint statistics, and considerable time was required for reconciling the discrepancies found. IPCC therefore decided to develop a new computer programme for more efficient verification of the two sets of statistical data. In May 2001, EDPS was engaged to develop a computer

programme for monitoring and verification of the complaint statistics (the “Matching Programme”).

## **Second Enhancement Programme**

4.5 In May 2003, since the CISS used by CAPO was undergoing enhancement which involved the addition of new codes and the revision of the existing codes, IPCC had to revise its system in order to allow CAPO’s data to be converted and retrieved in its own system. Again, EDPS was engaged to carry out this enhancement in January 2004 (the “Enhancement Programme”).

## **Maintenance Contracts**

4.6.1 IPCC also contracted EDPS for the maintenance of its computer statistical system. IPCC first engaged EDPS for maintenance of the system in November 1999 and the contract was renewed on an annual basis, and the last contract was in October 2005 (these contracts are collectively referred to as the “Maintenance Contracts” in this report).

4.6.2 All of the above contracts did not contain any general confidentiality clause nor did they require EDPS to take any measures to safeguard the security or further use of confidential information that were passed to them. The contracts did not contain any clause prohibiting EDPS from sub-contracting its services under the contracts.

4.6.3 At the material times, EDPS intended to sub-contract to Mr. Y all the maintenance and enhancement work it contracted with IPCC. In the first meeting with the staff of IPCC in 1998 at the IPCC’s office, regarding the development of the computer statistical system, the General Manager of EDPS introduced Mr. Y to the IPCC staff as the project manager. IPCC staff were given an EDPS business card bearing Mr. Y’s name with a job title of “Project Manager” (a copy of the business card can be found at Appendix V of IPCC’s report at Annex A). IPCC was unaware of the sub-contractual relationship between EDPS and Mr. Y. As far as IPCC was concerned, Mr. Y was an employee of EDPS. IPCC and its staff had ever since that time dealt with Mr. Y without knowing that there was a sub-contractual relationship between him and EDPS.

## CHAPTER FIVE

### Security and Privacy Policies

#### Security Policies

5.1.1 Both IPCC and CAPO operate in accordance with the Regulations of the Hong Kong Special Administrative Region, Volume 5, Security Regulations (the “Security Regulations”). In the Security Regulations, classified information are categorized in accordance with the degree of secrecy as “TOP SECRET”, “SECRET”, “CONFIDENTIAL” and “RESTRICTED”. The Security Regulations adopts a “need to know” principle that the dissemination of classified information should be no wider than is required for the efficient conduct of the business in hand and restricted to those who are authorized to have access. The principle shall be applied both within the government and in dealing with persons outside it.

5.1.2 In addition to the government-wide Security Regulations, IPCC issued an internal circular numbered 33/98 and titled “Departmental Security Instructions” (the “Security Circular”) to its staff in 1998. A copy of the Security Circular can be found at Appendix IV of IPCC’s report at Annex A. The Security Circular was circulated to IPCC’s staff every six months. By the Security Circular, IPCC expected its staff to follow the guidelines stated therein when handling classified documents. In the first paragraph of the Security Circular, the staff of IPCC were reminded of the sensitive nature of the files and investigation reports handled by IPCC, and that it was imperative that the security of these documents and information should be duly protected to guard against unauthorized disclosure.

5.1.3 In another internal circular numbered 37/98 and titled “Handling of Classified Documents”, staff of IPCC were reminded that all materials used to record classified material, including discs, must be treated as classified documents. A copy of this internal circular is at Annex B to this report. Apart from this, there were no specific written procedures or instructions given by IPCC to its staff regarding the handling of computer

discs or the transfer of data by electronic means.

5.1.4 CAPO classified all its files as “Restricted”. IPCC is of the view that the same level of security mentioned in the Security Regulations, the Security Circular and the internal circular numbered 37/98 are applicable to the complaint information contained in the computer discs given to it by CAPO.

### **Privacy Policy**

5.2.1 Apart from the Security Circular and the internal circular numbered 37/98 mentioned above, which provide general guidance on the handling of classified information, IPCC does not have its own privacy policy setting out matters such as the kind of personal data held by IPCC, the purpose of use of the personal data, the period for which the personal data would be retained, the staff designated to process request for access and correction of personal data, etc.

5.2.2 IPCC stated that in practice, the staff holding the post of that held by the then Supervisor was responsible for overseeing the overall compliance with the Ordinance, and that it was actively looking into the need of putting in place a policy document which would set out comprehensively its practices on personal data privacy and making it available to both its staff and the public.

## CHAPTER SIX

### Events Leading to the Leakage on the Internet

#### Introduction

6.1.1 In the course of this investigation, the Commissioner and his officers had examined extensively documents held by the various parties involved in the Incident and interviewed a number of witnesses.

6.1.2 This chapter describes the salient information obtained by the Commissioner and his officers.

#### Transfer of Data from IPCC to EDPS from May 2000 to May 2003

6.2.1 CAPO began providing computer discs containing actual information captured in CISS to IPCC in 2000. In or around May 2000, IPCC invited Mr. Y, the person it believed to be the employee of its IT contractor EDPS, to read the data on a computer disc furnished by CAPO but Mr. Y encountered difficulties. Mr. Y then advised IPCC to obtain another computer disc from CAPO with “denamenators” (special remarks to separate data of different fields from each other) added. On 12 June 2000, Ms. X of IPCC reported to the Deputy Secretary and the then Supervisor that the contractor had been engaged to read the computer disc prepared by CAPO and that she was informed by the contractor that it was quite difficult to read the data as the fields were not delineated. This event is evidenced by a file minutes of IPCC dated 12 June 2000. Based on Mr. Y’s advice, IPCC requested CAPO in writing on 26 June 2000 to provide another computer disc with denamenators added.

6.2.2 In or around May 2001, Mr. Y advised IPCC in connection with the Matching Programme that IPCC should ask CAPO for an up-to-date database so as to facilitate the data conversion process. This event is evidenced by a written record prepared by Ms. X on 24 May 2001. Pursuant to that suggestion, IPCC wrote on 25 May 2001 to CAPO for up-to-date CISS data stored in a computer disc. In or around June 2001, the disc containing actual complaint data was provided by CAPO to IPCC.

The disc was then given to Mr. Y by IPCC on the same day. This event is evidenced by a written record prepared by Ms. X on 12 June 2001. On 19 June 2001, Ms. X reported to the Deputy Secretary and the then Supervisor that the data provided by CAPO had been successfully decoded by Mr. Y. This event is evidenced by a written record dated 19 June 2001 prepared by Ms. X.

6.2.3 In the course of developing the Matching Programme beginning May 2001, Mr. Y conducted a trial run using “dummy” data. This event was recorded in the minutes of a senior staff meeting of IPCC held on 23 November 2001. Having completed the trial run by using “dummy” data, Mr. Y proceeded with a further trial by using actual data between end of 2001 and early 2002. This event was recorded in the minutes of another IPCC senior staff meeting held on 18 January 2002.

### **Transfer of Data from IPCC to EDPS from May 2003 to March 2006**

6.3.1 In May 2003, CAPO started to introduce enhancement to its CISS. This caused difficulties to Ms. X who could not read on the IPCC system the data from the disc provided by CAPO. She sought assistance from Mr. Y.

6.3.2 Mr. Y advised her that there were problems relating to the format and coding of the CAPO system. Ms. X arranged Mr. Y to contact the statistician of CAPO, who being a layman in IT matters, requested the Police Programmer to call Mr. Y direct to help solve the problems. This event was recorded in the minutes of an IPCC senior staff meeting held on 19 September 2003.

6.3.3 Mr. Y contacted the Police Programmer by phone on more than one occasion. He requested the Police Programmer to change the “variable length format” back to the original “fixed length format” to enable the IPCC system to read the CAPO data. The Police Programmer duly complied with such request.

6.3.4 In the course of their telephone conversations, the two IT professionals did not discuss the issues of testing environment and testing data. As stated by the Police Programmer, he merely elaborated on the

difference between the “variable length format” and the “fixed length format” he used on the computer programme. He himself never had access to live production data held by CAPO, which were protected by authorization and password.

6.3.5 In order to resolve the problem and to enable IPCC officers to read the data properly, the latest actual CISS data were handed over to Mr. Y for analysis. This event was recorded in the minutes of an IPCC senior staff meeting held on 14 November 2003.

### **Discrepancies between the Versions from IPCC and EDPS**

6.4.1 Crucial to this investigation are the discrepancies between the two versions put forward by Ms. X and Mr. Y, firstly as to whether or not Ms. X had expressly informed Mr. Y that the data given to him on the computer discs were actual confidential data; secondly, whether or not Mr. Y was aware of the confidential nature of the data; and thirdly, whether Mr. Y or EDPS had made an explicit request for IPCC to provide “test data” for the purpose of enabling IPCC to read the actual data supplied by CAPO.

6.4.2 Ms. X was involved in the IPCC Matching Programme in April 2001, the second Enhancement Programme in May 2003 and the annual Maintenance Contracts with EDPS. She asserted that she had no knowledge that Mr. Y was providing services as a sub-contractor of EDPS.

6.4.3 Ms. X could not recollect how many times and how many discs she had passed to Mr. Y, but she had no doubt that Mr. Y was fully aware of the nature of the data which were contained in the discs.

6.4.4 EDPS stated that the requests for “test data” were verbal, and that the discs containing the data were left at the IPCC reception counter for EDPS staff to pick up with no safeguards or warning whatsoever accompanying the discs, nor were there any requirements for acknowledgement of receipt by EDPS staff or undertaking from them to handle the data with care.



6.4.5 Ms. X recalled that on one occasion Mr. Y requested her to obtain from CAPO a computer disc containing updated data with “separators” between different fields. In this respect, Ms. X claimed that Mr. Y should know that the information contained in the disc was actual data held by CAPO.

6.4.6 Ms. X said that she had reported to her supervisors her every step taken with Mr. Y. The written records held by IPCC at least substantiate the following:

6.4.6.1 There was, in or around June 2000, a request from Mr. Y for CAPO to provide a computer disc containing the data, and the request was forwarded to CAPO on 26 June 2000;

6.4.6.2 Mr. Y asked, in or around May 2001, for an up-to-date database from CAPO so as to facilitate the data conversion process;

6.4.6.3 As requested by Mr. Y, a disc containing actual data was given to Mr. Y in or around June 2001, and subsequently the data were successfully decoded by Mr. Y;

6.4.6.4 As part of the Matching Programme, Mr. Y conducted a trial run by using “dummy” data. Mr. Y did another trial run using actual data between the end of 2001 and early 2002;

6.4.6.5 In or around September 2003, Mr. Y had direct discussions with CAPO and later the Police Programmer on the formatting of the CAPO data in the computer disc provided to IPCC; and

6.4.6.6 The latest actual CISS data were handed over to Mr. Y for analysis in or around November 2003.

6.4.7 Mr. Y said that he first became aware that the information

handled by IPCC concerned complaints against police officers during the Matching Programme in 2001. Although he had no idea what exactly the information was, he was aware that the data contained personal data, including names, dates, ages, addresses, etc.

6.4.8 Mr. Y claimed that in 2001 he obtained one computer disc from IPCC. On that occasion, Mr. Y attended the IPCC office after Ms. X had informed him by phone that the disc was ready for collection. He stated that Ms. X did not tell him what kind of information was contained in the disc. To his understanding, the disc contained data used for testing the Matching Programme. The disc was not given to him by Ms. X direct, but was handed to him by a member of IPCC staff at the reception counter. The disc was put inside a government envelope which had no markings of either “CONFIDENTIAL” or “RESTRICTED”.

6.4.9 EDPS stated in its written representations that:

*“As part of the development and testing process, a test environment was established and test data was requested from the IPCC. Testing environment, as the term suggests, is not necessarily free from programming bugs or security shortcomings. That is why testing data are normally computer-generated ‘dummy data’ or ‘sanitized’.”*

6.4.10 EDPS maintained that it did not know the confidential nature of the data provided by IPCC.

6.4.11 The issue of “test data” and whether Mr. Y was aware that the discs provided by IPCC contained actual live data as opposed to “dummy” data will be further discussed in chapter seven of this report.

### **Leakage of the Complainants’ Personal Data on the Internet**

6.5.1 According to Mr. Y, the “test data” obtained from Ms. X were stored in his notebook computer and his computer at home. After the completion of testing the second Enhancement Programme, Mr. Y installed the programme into the IPCC computer statistical system at the

IPCC office in early 2004. Some time after the installation in early 2004, Mr. Y uploaded the completed source programme with all materials including the “test data” he used for developing the IPCC second Enhancement Programme onto the server of a company known as China Motif Limited, which also hosted the Website.

6.5.2 The Website was set up by Mr. Y and Mr. Y’s Partner for the purpose of sourcing merchandise in mainland China for sale in Hong Kong and was registered in the name of the Webmaster.

6.5.3 The Webmaster stated that Mr. Y was his former colleague who later set up his own business and contracted part-time jobs to the Webmaster. The Webmaster designed and maintained the Website for Mr. Y. Mr. Y was permitted and able to upload information or material onto the Webmaster’s server independently.

6.5.4 According to the Webmaster, the information leakage of IPCC data was caused by Mr. Y, who had uploaded the confidential information of IPCC to a location of the server, which was accessible by others. Mr. Y might not have realized that uploading information to different locations of the server would have different effects. Mr. Y had never asked the Webmaster the location or sub-directory in the server whereby access by others through the Internet might be possible, and the Webmaster had not advised Mr. Y of the same.

6.5.5 The IPCC data surfaced on 10 March 2006 when a member of the public while searching on the Internet stumbled across names, addresses and identity card numbers of complainants via the Website.

6.5.6 The technical stance of EDPS is as follows:

*“The way of the test data was stored, as we now know, has been compromised by a combination of numerous system tools, search engines, and the Internet, even though the test data was stored in a private server, which was used only for testing and internal purposes, protected by user-id and password and accessible by only a few technicians. This problem is of a technical nature and is contained entirely within the testing environment. It can*

*easily be remedied without serious consequences if indeed the data in question is the test data as it should be.”*

## **Other Witnesses**

### The then Supervisor

6.6.1 The then Supervisor was the immediate supervisor of Ms. X. He claimed that he only knew some basic principles of the IT programmes of IPCC but did not know the details. In the course of developing the IT programmes, the then Supervisor did not receive any instructions from his seniors to provide assistance to EDPS, and Ms. X had not consulted him on this aspect.

### Mr. Y’s Partner

6.6.2 Mr. Y’s Partner was aware that Mr. Y had some on-going maintenance job with IPCC but he was not told of the details of the job. Mr. Y’s Partner had no idea that Mr. Y had uploaded IPCC’s database onto the server hosting the Website.

## CHAPTER SEVEN

### The Commissioner's Findings

#### The Commissioner's Findings against IPCC

7.1.1 DPP4 as referred to in paragraph 1.1.3 of this report requires a data user to implement security safeguards and precautions in relation to the personal data in its possession. The security level should reflect the sensitivity of the data and the seriousness of the potential harm that may result from a security breach.

7.1.2 The present case concerns the arrangement of outsourcing the development, enhancement and maintenance of a computer database system by a data user (IPCC) to a contractor (EDPS) who assigned the jobs to a sub-contractor (Mr. Y) without the knowledge of the data user (IPCC). The contractor (EDPS) was expected to examine the data concerned and test run the system with the data before delivering the products to the data user (IPCC).

7.1.3 For the purposes of carrying out the outsourced work, Mr. Y asked IPCC to provide him with the data involved. From the evidence before me, I do not find that IPCC had given any due consideration to ensuring security of the data.

7.1.4 The Security Circular issued by IPCC to its staff stated that: *“In view of the large number of CAPO case files and investigation reports, which are of a sensitive nature, handled by the IPCC Secretariat, it is imperative that the security of these documents/information should be duly protected to guard against unauthorized disclosure.”* It is clear that IPCC was fully aware of the sensitivity of the data it was handling. Leakage of such data would not only cause acute anxiety to those affected but also give them grave concerns on their personal safety. Conceivably, if fallen into the wrong hands, the data might be used in such fraudulent activities as impersonating those affected in obtaining credit from financial institutions. Given the sensitivity of the data and seriousness of the harm that could result from a leakage of the information, great

caution and sufficient safeguard should have been taken by IPCC to protect the data in all circumstances, in particular when being asked to release the data to a third party, such as the contractor in the Incident.

7.1.5 The contractual relationship between EDPS and IPCC can be traced back to 1998. With clear understanding of the nature and scope of the tasks outsourced to EDPS, IPCC ought to have known that data were required for testing the system by the contractor. Indeed, from the copies of written records prepared by Ms. X dated 12 June 2000, 12 June 2001 and 19 June 2001, and the minutes of IPCC's senior staff meeting held on 18 January 2002, it is apparent that IPCC was at the time fully aware that actual data of the CAPO cases were released to Mr. Y.

7.1.6 Ms. X as the responsible officer and/or her supervisors did not give any consideration as to whether they should release actual data or "dummy" data to Mr. Y. It appears that Ms. X presumed that it was necessary to give actual data to the contractor and no mention was made in her dealings with Mr. Y on the feasibility of using "dummy" data. In response to my inquiries during this investigation, EDPS and Mr. Y both stated that they did not need actual data from IPCC for testing the programme. IPCC had since the leakage agreed that "dummy" data could have been used for testing the programme or system enhancement by EDPS. If due consideration was given at the time on the use of "dummy" data, the Incident might conceivably have been avoided.

7.1.7 In view of the sensitive nature of the data involved, it would be ideal if the actual data did not have to leave IPCC's premises. However, I cannot find any evidence that Ms. X or indeed anyone in IPCC had, before releasing the data to Mr. Y, discussed with him or considered whether the process in which actual data were to be used could be carried out within IPCC's premises.

7.1.8 The then Supervisor claimed that no one was allowed to take the confidential data of CAPO outside the IPCC office and that Ms. X should understand this on reading the Security Circular. Ms. X confirmed that she had read the Security Circular but did not consider its contents prohibited her from releasing actual data to the contractor. Upon a reading of the Security Circular I am inclined to agree with her. If it was

IPCC's policy not to allow CAPO data to leave its office as claimed by the then Supervisor, I cannot find any solid evidence which shows that clear instructions had been given by IPCC to its staff in this respect.

7.1.9 It was within reasonable expectation that the personal data would be required for testing the system at some stage. However, IPCC had not issued any practical guidelines to its staff in respect of the matters that needed to be considered if a request for personal data was made by its contractor. There was also no guidelines issued by IPCC alerting its staff of the privacy risks involved if any of the sensitive data were to leave its office and its control.

7.1.10 I accept that, depending on the complexity of the job and other consideration (such as the level of accuracy required for a test), there could be situations where the use of actual data might be required by the outsourced contractor in the process of developing and maintaining a computer database system. In such circumstances it might be necessary to release the actual data to the contractor for processing outside the data user's premises. Before releasing the data, the data user must take all practicable precautionary measures to prevent leakage of the data by the contractor. There is no evidence which shows that IPCC had taken any practicable precautionary measures to prevent leakage of the data by EDPS or Mr. Y.

7.1.11 In a service contract that involves the handling of personal data by an outsourced contractor there should be a clause imposing on the contractor the obligation to keep the personal data secure and confidential. I do not find the inclusion of such a clause in any of the service contracts between IPCC and EDPS. Nor do I find in any of the service contracts an imposition of obligation requiring EDPS to take security measures to protect the sensitive personal data entrusted to it by IPCC.

7.1.12 DPP4 requires a data user to take measures for ensuring the integrity, prudence and competence of persons having access to the personal data held by it. The evidence available to me shows that IPCC's complaint information was leaked as a result of an act done by Mr. Y. Whether or not IPCC had exercised due diligence when selecting EDPS as its contractor, its failure to incorporate into its service contracts

with EDPS a prohibitive clause restricting EDPS's power to sub-contract the services created a risk that the sensitive data might be released to a person whose integrity, prudence and competence were unknown to IPCC and over whose conduct IPCC would have no control.

7.1.13 Having considered the above and all the circumstances of the case, I find that IPCC had failed to consider in the first place whether it was necessary to part with the personal data received from CAPO before releasing the data to Mr. Y. I also find that IPCC in releasing the data to Mr. Y had failed to take any precautionary measures, contractual or otherwise, to safeguard the data from unauthorized or accidental access having regard to the highly sensitive nature of the data concerned. I further find that in the Incident IPCC had not taken any practicable steps to ensure the integrity, prudence and competence of the person or persons who would be given access to the data.

7.1.14 In view of the foregoing, I find that IPCC had contravened the requirements of DPP4.

### **Comments on the Parts Played by Other Parties in the Incident**

7.2 The leakage of the personal data on the Internet in the Incident was caused by Mr. Y uploading the data onto the server hosting the Website. The leakage might have been avoided if IPCC had duly complied with the requirements of DPP4 in handling the outsourcing arrangement. Other parties are also involved in the Incident and public interest would expect me to make comments on them and Mr. Y in respect of their respective roles and conduct in relation to the personal data concerned.

### ***Comments relating to CAPO***

7.3.1 In view of the monitoring role of IPCC, CAPO was obliged to provide the complaint information to IPCC. I also note that to allow IPCC to carry out research and prepare statistics effectively, it is necessary for IPCC to obtain comprehensive complaint data from CAPO in electronic form. Nevertheless, to minimize the risks of leakage and misuse, such release of electronic data by CAPO should be limited to



those data that are required for the research and statistical purposes.

7.3.2 It would have been sensible for IPCC and CAPO to review the categories of data to be provided by CAPO to IPCC, having regard to the purposes for which the data were to be used. I suggest IPCC and CAPO do consider (if they have not already done so) whether it is necessary for CAPO to transfer to IPCC for research or statistical purpose individuals' identifying particulars like identity card numbers, police officer numbers, full names and addresses.

### ***Comments relating to EDPS***

7.4.1 EDPS confirmed that when its representative first visited IPCC's office together with Mr. Y to solicit the first service contract, the staff of IPCC were given an EDPS business card bearing Mr. Y's name with a job title of "Project Manager". On this occasion, neither EDPS nor Mr. Y told IPCC that if given the job EDPS would only be the contractor and Mr. Y would be the sub-contractor doing the actual work. EDPS and Mr. Y might or might not have intended it, at that meeting and ever after, an impression was created on IPCC that the work given to EDPS would be undertaken by Mr. Y as an employee of EDPS and that EDPS would be the only party responsible for the work concerned. While EDPS was not prohibited from sub-contracting any of the IPCC contracts to a third party, it would be good practice for EDPS to make it clear from the outset that Mr. Y was its intended sub-contractor, or, after it was given the jobs, inform IPCC of the sub-contracting arrangement. From the perspective of data security, if IPCC had been made aware that the projects were handled by a sub-contractor, IPCC might have given due consideration to the issue of data security associated with the handling of sensitive personal data by a sub-contractor.

7.4.2 EDPS claimed that Mr. Y had only asked for "test data" from IPCC, and that it was impossible for EDPS to create data for testing in the projects. EDPS however did not explain to IPCC that "test data" meant "dummy" or sanitized data. Although EDPS claimed that any IT professional should have no difficulty in understanding the meaning of the term "test data", they had not taken any steps to ensure that Ms. X, who was a non-IT professional, understood the term.

7.4.3 According to Mr. Y, the guidance provided to him on data security by EDPS was limited to some verbal instructions on keeping clients' data confidential. EDPS claimed that there was an understanding between it and Mr. Y regarding the duty to keep confidential clients' data and that such understanding had been reduced in writing in its contract with Mr. Y. When asked to produce a copy of the contract to my Office, EDPS was unable to do so. I am not convinced that EDPS did provide sufficient guidance to Mr. Y in relation to the handling of the data collected from IPCC, nor am I convinced that EDPS established any policy or procedure on the return or disposal of the data, "test data" or otherwise.

### ***Comments relating to Mr. Y***

7.5.1 Mr. Y should be aware that he was mistaken by IPCC as a member of EDPS's staff and not as an independent sub-contractor. It is remarkable that at no time did Mr. Y take steps to correct that wrongful impression.

7.5.2 Consistent with the representations of EDPS, Mr. Y claimed that he merely asked Ms. X for "test data", a term which he said meant, in the IT parlance, data which were not real. Ms. X said that she sought help from Mr. Y whenever she encountered difficulties in reading the CAPO discs. Since she had problems reading the discs, she could not be expected to be technically capable of providing "dummy" or sanitized data in the enhanced CISS format to Mr. Y. Mr. Y or EDPS could not reasonably expect "dummy" or sanitized data from Ms. X or IPCC without their guidance or assistance. As Mr. Y was dealing with a non-IT professional, a more prudent person would have been concerned to see whether the term was understood properly and whether some explanation or discussion was necessary to ensure that there be no misunderstanding.

7.5.3 Throughout my investigation, I was perturbed by the manner in which IPCC's data was handled by Mr. Y. First, he had not given any receipts to IPCC in respect of the discs or the data obtained by him from Ms. X or IPCC. Secondly, I do not find any log or record kept by Mr. Y

in respect of his receipt of the discs or the data from Ms. X or IPCC. Thirdly, I do not find any written record from him of his uploading of the data onto the server of his company. Fourthly, there was no discussion between Mr. Y and Ms. X about the return or disposal of the discs or the data after use by Mr. Y. Fifthly, I do not find any record from Mr. Y of the destruction of the discs or the data. Lastly, Mr. Y had not given any written notice to IPCC advising or confirming the destruction of the discs or the data.

7.5.4 It might well be claimed by Mr. Y and EDPS that it had treated the IPCC data as “test data”. Nonetheless, having heard all the evidence and submissions, I am not convinced that Mr. Y was not aware that the data given by IPCC were actual data of CAPO’s cases. Even if he in fact was not so aware, he did not seem to have taken any steps to protect the data, be they “test data” or not, from unauthorized or accidental access by uploading them onto a server connected to the Internet which was accessible to the public. Obviously, Mr. Y had not given any consideration to the consequence or effect of putting the data on the server.

### ***Comments relating to Ms. X and her then Supervisor***

7.6.1 Written records of IPCC showed that Ms. X, who was not conversant nor trained in IT matters, had habitually reported to her then Supervisor and other senior staff about how the CAPO data were handled, and that actual data from CAPO were on various occasions forwarded to Mr. Y. Based on these records and after listening to the testimony of Ms. X given on oath, I have no reason to doubt the truthfulness of her account of the events in respect of her encounters with Mr. Y.

7.6.2 According to IPCC’s practice (see paragraph 5.2.2 of this report), the then Supervisor was responsible for overseeing the overall compliance with the Ordinance. I am very surprised that the then Supervisor, being the immediate supervisor of Ms. X, claimed that he did not know the details of the outsourced computer projects handled by Ms. X and that his knowledge on the projects and on IT systems was limited to some basic principles. I am not impressed by his want of awareness of the project progress, despite the fact that Ms. X had maintained records

on files and reported in meetings over the years in respect of her dealings in the projects. In addition, the then Supervisor had not sought to ensure that:

- (i) receipts be obtained from Mr. Y or EDPS for of the discs and the data passed to them;
- (ii) log records of every transfer of data to Mr. Y or EDPS were kept;
- (iii) written instructions were given to Mr. Y or EDPS to keep the data secure and confidential;
- (iv) there be discussions and due consideration as to whether the discs or the data should be returned or destroyed after use by Mr. Y or EDPS;
- (v) Mr. Y or EDPS be required to return or destroy the discs or the data within a specific period of time;
- (vi) if the discs or the data were to be destroyed by Mr. Y or EDPS, written confirmation or report be obtained from Mr. Y or EDPS on details of such destruction once it was carried out.

This is unsatisfactory in view of the then Supervisor's position being the immediate supervisor of Ms. X and the officer responsible for personal data matters in IPCC.

7.6.3 It appears to me that Ms. X was almost left alone within the IPCC organization to handle the computer projects without much guidance and supervision. I consider that the problem was partly attributable to the inadequate supervision given to Ms. X from her then Supervisor and the IPCC management during the process and the lack of proper training and support to Ms. X, both in terms of handling sensitive personal data and IT knowledge.

### ***Comments relating to the Webmaster***

7.7 The Webmaster was engaged by Mr. Y and Mr. Y's Partner to set up the server supporting the Website as well as the computer system of Mr. Y's company. It is the Webmaster's belief that the information leakage was caused by the uploading of the confidential information of

IPCC by Mr. Y to a location of the server where the public could have access. It is apparent that Mr. Y did not know this beforehand. It is arguable that the information leakage might have been avoided if the Webmaster had warned Mr. Y that uploading information to certain locations of the server would cause the information vulnerable to public access. I am concerned that the Webmaster failed to inform Mr. Y, the end-user, such important features of the server.

## **CHAPTER EIGHT**

### **Actions Taken by IPCC after the Leakage and Recommendations by the Commissioner**

#### **Actions Taken by IPCC after the Leakage**

8.1 Subsequent to the information leakage, IPCC has carried out certain measures including the following:

- (i) its Chairman made open apologies to the public on 11 and 17 March 2006;
- (ii) set up telephone hotlines to answer public enquiries in respect of the Incident;
- (iii) set up three sub-committees headed by the Chairman and two Vice-chairmen to meet members of the public who have expressed concern about the Incident;
- (iv) sent letters of apology to those affected by the leakage;
- (v) continue to carry out cyber patrolling together with the Commercial Crime Bureau of the Police to thwart abuse of the leaked information on the Internet;
- (vi) appealed to Google and other search engine companies to erase the leaked information stored in the cache in order to stop the circulation of the leaked information on the Internet;
- (vii) upgraded its computer system to support enhancement of security functions;
- (viii) appointed a full time IT professional to enforce system data security control and related matters; and
- (ix) proceeded to appoint an independent consultant to carry out an IT security risk assessment on its computer system.

## **Enforcement Notice**

8.2.1 Pursuant to section 50 of the Ordinance and in consequence of my investigation, if the data user being investigated is found to be contravening a requirement of the Ordinance or has contravened such requirement in circumstances that make it likely that the contravention will continue or be repeated, I may serve on the data user an enforcement notice directing it to carry out specific steps to prevent future repetition of the contravention.

8.2.2 Despite the above measures taken by IPCC, I am of the view that the contravention of DPP4 on the part of IPCC will likely continue or be repeated. My opinion is based on the fact that IPCC did not have any practical policy or guidelines in place for staff to follow in respect of the matters that needed to be considered when handling request for the complaint data by an outsourced contractor or agent; the precautionary measures that have to be taken in the event that it is necessary to release the complaint data to an outsourced contractor or agent; and the measures for ensuring the integrity, prudence and competence of the persons who might have access to the data in an outsourcing arrangement.

8.2.3 In exercising my powers under section 50 of the Ordinance, I have also taken into account that the leakage had caused damage or distress to the individuals whose personal data were exposed on the Internet. Accordingly, I have issued an enforcement notice to IPCC directing it, in effect, to:

- (i) devise the necessary policy and practical guidelines for the proper handling and protection of the complaint data when dealing with an outsourced contractor or agent;
- (ii) implement effective measures to ensure compliance by its staff with those policy and guidelines; and
- (iii) review the existing outsourcing contracts and endeavor 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.

## **Recommendations Arising from the Investigation**

8.3.1 The Incident revealed the lack of awareness of protecting personal data by the data user and the IT practitioners entrusted with sensitive personal data. I am also concerned about the common practice for organizations to outsource the development or maintenance of computer systems, which often involves the transfer of staff or customer personal data to an outsourced contractor or agent.

8.3.2 Learning from this unfortunate Incident, it is paramount for data users to take precautionary measures in the event that they find it necessary to release database containing personal data to an outsourced contractor or agent. Furthermore, more effort is required to raise the sensitivity of IT practitioners and government officers on the protection of personal data.

### ***Measures to be Taken when Engaging Outsourced Contractor or Agent***

8.4.1 It is recommended that considerations be given to the following before any personal data are released to an outsourced contractor or agent:

- (i) sensitivity of the personal data and the harm that could result in the event of a leakage;
- (ii) necessity to use “actual” personal data after proper enquiries and discussion with the outsourced contractor or agent of the use of “dummy” data instead;
- (iii) the risks involved in releasing personal data; and
- (iv) where the use of “actual” personal data by the contractor or agent is necessary, whether it is feasible to carry out the required procedures within the premises of the organization.

8.4.2 If it is considered necessary to release “actual” personal data to an outsourced contractor or agent, the following precautionary measures should be taken:

- (i) select a reputable contractor or agent offering guarantees



- on their ability to ensure the security of the personal data;
- (ii) incorporate into the terms of the service agreement the following:
    - (a) prohibiting the contractor or agent to use or disclose the personal data for a purpose other than the purpose for which the outsourced contractor or agent is assigned to carry out;
    - (b) security measures required to be taken by the contractor or agent to protect the personal data given to them and obliging the contractor or agent to protect the personal data by complying with the data protection principle of the Ordinance;
    - (c) requiring a timely retrieval or return of the personal data when they are no longer required for the purpose for which the contractor or agent is assigned to carry out;
    - (d) absolute or qualified prohibition against sub-contracting the service concerned;
    - (e) requiring immediate reporting of any sign of abnormalities or security breaches by the contractor or agent; and
    - (f) measures required to be taken by the contractor or agent to ensure that its staff who handle the personal data will carry out the security measures and comply with the obligations under the service agreement regarding the handling of personal data;
  - (iii) audit the contractor or agent from time to time to confirm if it is carrying out the required security measures and obligations;
  - (iv) keep proper records of all the personal data that have been transferred to the contractor or agent;
  - (v) give clear instructions to the contractor or agent in respect of the use, transmission, storage and destruction of the personal data; and
  - (vi) seek approval from the senior management of the organization before releasing database containing personal data to the outsourced contractor or agent.

### ***Recommended Practice for IT Practitioners***

8.5.1 In order to enhance awareness of and provide guidance to IT practitioners in protecting personal data in their daily work, I find it necessary to devise practical guidelines outlining the professional responsibilities of IT practitioners and provide guidance for others when using IT systems that contain or will be used for processing personal data. My Office together with leading IT organizations will jointly issue a set of guidelines titled “Recommended Procedures for IT Practitioners on Personal Data”.

8.5.2 It is recommended in the guidelines that the following practices be adopted by IT practitioners when handling personal data:

- (i) state and define functional responsibilities of different levels of IT personnel in protecting personal data. For instance, system development staff should ensure that no personal data are used for system diagnosis or bug-tracking, and database administration staff should document all applications that access personal data in the database;
- (ii) all access to personal data database, copy/backup from the database, and image exported from the database should be authorized, monitored and accounted for, and reports on these database operations should be produced and reviewed regularly;
- (iii) prominent notice should be generated whenever an end user accesses an IT system that contains personal data, and end users of an IT system should not export or save any personal data from the system unless formally approved;
- (iv) export of personal data should be authorized and exported data on removable storage media, e.g. floppy diskettes, CDs, USB drives should be properly labelled. Computer printouts that contain personal data should contain proper labels and emails that contain personal data should have the content encrypted and properly labelled;
- (v) destroy the personal data which are no longer in use. For personal data stored in a personal computer, the computer hard disk should be sanitized; for personal data in a server,

- the server's hard disk should be sanitized; all backup copies and printed copies should be destroyed and proper records should be kept of the destructions; and
- (vi) carry out audit from time to time on the creation, access, modification, and destruction of any personal data stored in electronic media.

8.5.3 Apart from the promulgation of the guidelines, seminars will be held in which IT practitioners may share best practices and experience on data protection. Appeals will also be made to all local higher educational institutions to include data privacy into the curriculum for IT subjects.

### ***Guidance to Government Officers***

8.6.1 I am particularly concerned about the handling of personal data by government departments which hold a large amount of personal data of the public. I recommend all government departments to include a particular topic on the requirements of the Ordinance as part of their regular training to staff and provide practical guidance on compliance with the Ordinance.

8.6.2 As a move to enhance the awareness of data protection in government departments, my Office together with the Home Affairs Bureau are planning to organize seminars on compliance of the Ordinance for government officers.