



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

**The Work Report of the Privacy Commissioner,
Roderick B Woo**

December 2009

Table of Content

Page	
My Review	1
Work Report	
Chapter 1: The Ordinance and the Establishment of PCPD.....	7
Chapter 2: PCPD’s Promotional Activities.....	11
Chapter 3: Educational Initiatives	20
Chapter 4: Guidance Work	24
Chapter 5: Compliance Work	30
Chapter 6: Enforcement Work.....	50
Chapter 7: Law Reform	54
Chapter 8: Global Liaison and Cooperation	61
Chapter 9: The Efficient Utilization of Resources by the Commissioner	70
The Way Ahead	73

My Review

Genesis

I was appointed Hong Kong's Privacy Commissioner to protect the privacy of individuals in relation to their personal data. I have now served all but seven months of my five-year term. It is time for an end-of-term report so that the public is properly informed of the work that has been done and what I consider has yet to be done.

The first nine months of my term had been a very trying time for me. As a new chief I had to work without a deputy while attending to an unhappy situation left behind by a former deputy commissioner. It was also during this period that I had to see to the office relocation as the old tenancy expired.

Scope of Work

The Personal Data (Privacy) Ordinance ("the Ordinance") sets out my functions which include (1) promotion of privacy awareness; (2) education in relation to protection of privacy; (3) guidance to the public on the handling of personal data; (4) checking compliance with the requirements of the Ordinance; (5) investigation and enforcement in respect of complaints received and where a suspected breach is brought to my attention; (6) handling legal cases; (7) law reforms and (8) working on international and regional levels.

In the performance of my duties I have always borne in mind the essential goals of raising privacy awareness and promoting good privacy governance among organizational data users.

To Create the Right Setting

As soon as I had settled down, I decided to create the right setting and condition in which the work of protecting personal data can best be done. Among my efforts was the review of the Ordinance in order to bring about an updated piece of privacy legislation that adequately protects personal data. With this objective in mind, I set

up an internal working group to review the Ordinance. After a year and half the working group, which performed the job of a law reform committee, presented to the Government more than 50 amendment proposals. The Constitutional and Mainland Affairs Bureau, after careful consideration of the proposals indicated that the Government agreed in principle to most of them. It has in fact published a Consultation Document inviting public comments. Hong Kong can now look forward to an updated and improved edition of the law that protects personal data privacy to meet new threats posed by the rapid developments in information technology.

I have also caused the publication of *“Data Protection Principles in the Personal Data (Privacy) Ordinance - from the Privacy Commissioner’s perspective”*. This is still the only reference book of its kind giving the readers and data protection officers an insight into the actual application of the data protection principles which form the cornerstone of our privacy law.

Operational Constraints

Considering the variety of functions and the large number of stakeholders concerned, my Office is indeed small in terms of manpower and monetary resources. From its inception thirteen years ago, the number of officers entrusted to perform these functions averages less than thirty excluding the basic administrative staff. Take for instance, the officers in the Operations Division who handle all the incoming complaints hardly ever exceeded ten in number over the years. This is to be measured against the fact that the scope of the application of the Ordinance, the conduct regulated thereunder and the people affected by it, are profound and far reaching.

The “Selective to be Effective” Approach

Against this background of multiple functions and scarcity of resources, I have to face the stark reality that the number, nature and complexity of the complaints received are totally unpredictable and that I have no control over what serious data breach may occur in society from moment to moment. Experience has taught me that rigid pre-meditated planning does not work well in practice and I have to be selective in order to be effective.

The challenge lies in selecting the work that merits priority of attention and treatment. I shall briefly recount what I have selected and what success I think I have achieved.

(i) Pro-active Attitude

In 2006 I set up the Compliance Division to carry out checks on data users to see if they are complying with the Ordinance, particularly in cases which have caused community concerns or which have a serious impact on data privacy. The Compliance Division has now become an effective arm of the Privacy Commissioner's investigation and enforcement unit.

In May 2008, Hong Kong was appalled by a spate of unauthorised disclosures of patients' medical data in several public hospitals. It was then that I decided to invoke for the first time the statutory power of Inspection to critically examine the Hospital Authority's patients' data security system. With the kind co-operation of four eminent volunteers, I was able to present a report to the Hospital Authority within 3 months. I was gratified by the Hospital Authority's total acceptance of the 37 recommendations that were presented to it.

(ii) No Waiting

Investigations which I have decided to make without waiting for a complainant to come along included the well publicized leaks of the personal data of thousands of citizens who had complained against individual police officers; the covert surveillance of its employees by a post office via pin-hole cameras; a bank's loss of a server containing numerous data of its customers; the unauthorised disclosure on the internet through share file software of documents containing personal data kept by a government department. I was grateful that these and other self-initiated actions have proved fruitful and were appreciated by the public.

(iii) Participation in Civic Projects

Before the introduction of the current Hong Kong Smart ID cards in 2003, the Privacy Commissioner gave advice to the Privacy Impact Assessments for the Immigration Department at its request, and right now as I am writing my Office is carrying out a

Privacy Compliance Audit for the same Department also at its request to check if everything is in ship shape condition.

I have participated in many public programmes including the pilot scheme of drug tests in schools. Of late, I have indicated my willingness to support and work with the Government on the eHealth Recording Sharing Programme.

(iv) Risk Management

My time and efforts are concentrated on issues that have a significant impact on the overall personal data privacy situation. This generally satisfies the public's just demand and has the added advantage of capturing its attention, making it easier for me to convey my message. I also target malpractices that may seriously affect the social and/or economic well-beings of Hong Kong and its people. My strategy is led by risk-management with a view to achieving the greatest promotional and regulatory effect with the least resources.

All these jobs mentioned above were done without any pre-arranged allocation of funds. They were done because they had to be done in answer to the demands and needs of the public at the time, and if I had to dip into my reserve fund, I would have done so with bold prudence. The subsequent acknowledgement by the Government that it supports the establishment of the Compliance Division and that it expects the Privacy Commissioner to regularly exercise the power of Inspection show that my selective approach is effective.

Accountability

In whatever I do and decide, I hold myself out to be accountable to the public, the courts, the Administrative Appeals Board, the Legislative Council and the Ombudsman. The use of the public fund at my disposal is constantly subject to the oversight of the Constitutional and Mainland Affairs Bureau, by our external auditors and Audit Commission. I have always been conscious of the need to exercise care in spending public money and during my tenure have achieved a degree of saving in expenditures previously not attained.

Transparency

Maximum permissible transparency is my other guiding principle. I regularly brief the public through the media on the work and development of my Office. I report through annual reports, newsletters, investigation reports and case notes. Frequently have I issued public statements setting out my stance and views on topical privacy issues. The latest news is uploaded in real time to my official website for all to see.

International Attention

My efforts have not escaped international attention. The following opening lines in the UK based publication "Privacy Laws and Business International Newsletter" in June 2008 reflect the challenges that face me,

"It is not easy these days being Hong Kong's Privacy Commissioner. In the first five months of this year, Hong Kong has been rocked by revelation of dozens of data leaks and losses, including those of confidential government information, hospital and banking records.....Privacy Commissioner Roderick B. Woo, who oversees Hong Kong's implementation of the Personal Data (Privacy) Ordinance, has issued at least 15 public statements dealing with the incidents, appeared before the Legislative Council and, for the first time, invoked his office's power to inspect personal data systems....."

Gratitude and Prayers

I have indeed dealt with many privacy issues, much more than anyone had anticipated four and half years ago. Through it all, I have gladly taken on all the challenges and I enjoy serving the public as its privacy guardian. I am grateful for the supports that have been given me by my colleagues, by the Government, by the media and by friends, organisations and individuals who seriously care about the protection of the individuals' right to personal data.

I fervently pray that the Government and the community at large will recognise the positive contributions to society brought about by the Ordinance and the work of this independent personal data protection authority, and will not fail in their support to the continuing work of the Privacy Commissioner for Personal Data.

Roderick B WOO
Privacy Commissioner for Personal Data
December 2009

Work Report

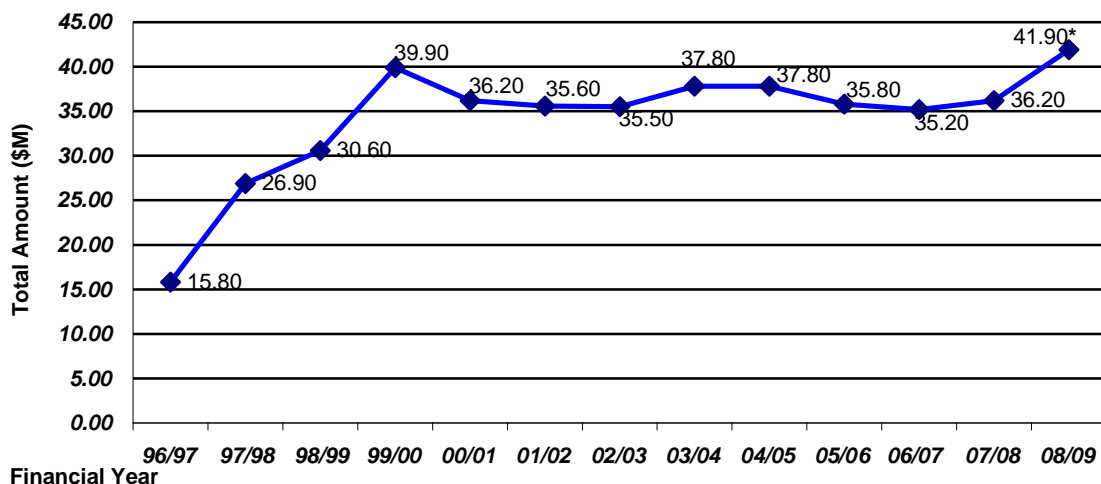
Chapter 1: The Ordinance and the Establishment of PCPD

The enactment of the **Personal Data (Privacy) Ordinance** (“the Ordinance”) is the recognition of the basic right of personal data privacy by the Hong Kong SAR Government. It is a significant and far-sighted step in the history of human right and information development. It fosters and consolidates cross-border data flow, and confirms the status of Hong Kong as a jurisdiction that has personal data privacy protection legislation in the world.

The Ordinance aims to provide protection on personal data privacy. An office by the name of the **Privacy Commissioner for Personal Data** (“the Commissioner”) is established under the Ordinance. The Commissioner is appointed by the Chief Executive to perform the functions and exercise the powers conferred by the Ordinance to protect personal data privacy. The **Office of the Privacy Commissioner for Personal Data** (“the PCPD”) is an independent regulatory organization headed by the Commissioner. All data users, no matter individuals, public or private organizations, are subject to the jurisdiction of the Ordinance.

The operating resources of the PCPD mainly come from government subvention annually. Since the establishment of the PCPD 13 years ago, the amount of fund each year ranges between 30M and 40M (see **Fig. 1**).

Fig. 1: Government Subvention to the PCPD



*Excluding \$1,000,000, being one-off subsidy for the year granted on promotional projects by the Government.

Apart from administrative staff, the average manpower of the PCPD since its establishment was below 24 (see **Fig. 2**). There is no significant increase over the years. It was increased to 29 only in 2008/09.

Fig. 2: Permanent Staff Establishment of the PCPD

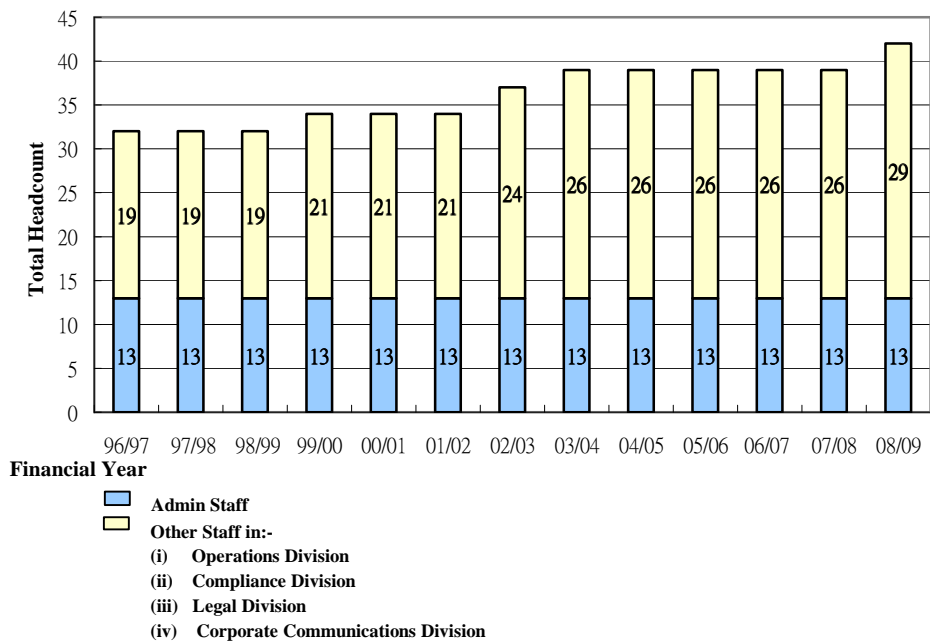


Fig. 3 illustrates the bids made to the Government for increasing the establishment posts since the establishment of the PCPD. The figures show that the average successful rate of granting the additional posts applied for is about 12%.

Fig. 3: RAE bids submitted by PCPD to the Controlling Officer from 1998 to 2009

Year of Application	Bid	Result	Year of Allocation
1998	Bid for creation of 23 posts for Operations, Legal, Administration and Corporation Communications Divisions and for carrying out inspection and handling information infrastructure	Rejected	
1999	Nil submission		
2000	Nil submission		

Year of Application	Bid	Result	Year of Allocation
2001	Bid for creation of 18 posts for Operations, Legal and Corporate and Communications Division <i>(Fund bid for: 15.807M)</i>	13 posts rejected. Funds for 5 posts granted (i.e. 1 Chief Personal Data Officer, 2 Senior Personal Data Officers and 2 Personal Data Officers in Compliance Division) <i>(Fund granted: 4.778M)</i>	i) 2002-03: 2.495M ii) 2003-04: 2.283M
2002	Nil submission		
2003	Nil submission		
2004	Nil submission		
2005	Bid for creation of 4 posts for Legal and Policy Divisions and for carrying out inspection exercise	Rejected	
2006	Bid for creation of 19 posts for Compliance Team	Rejected	
2007	Bid for creation of 12 posts for Compliance Team <i>(Fund bid for: 9.317M)</i>	9 posts rejected. Funds for 3 posts granted (i.e. 1 Personal Data Officer, 1 Assistant Personal Data Officer and 1 Assistant Personal Data Officer (IT)) <i>(Fund granted: 1.84M)</i>	2007-08
2008	<ol style="list-style-type: none"> 1. Bid for creation of 11 posts for Compliance Division to undertake inspection and compliance investigation 2. Bid for creation of 11 posts to step up services in Ops Division and in preparation for undertaking prosecution works 3. Bid for creation of 4 posts to step up services in Legal Division 4. Bid for creation of 3 posts in Corporate and Communications Division for promotion of awareness of PDPO 5. Bid for creation of 2 posts for IT Team <i>(Total fund bid for : 22.635M)</i>	<p>7 posts rejected. Funds for 4 posts granted (i.e. 1 Chief Privacy Compliance Officer, 1 Senior Personal Data Officer and 2 Personal Officers) <i>(Fund granted: 3.618M)</i></p> <p>Rejected</p> <p>Rejected</p> <p>Rejected</p> <p>1 post rejected. Funds for 1 post of IT Adviser granted <i>(Fund granted: 1.382M)</i> <i>(Total fund granted: 5.0M)</i></p>	<p>2009-10: 3.618M[△]</p> <p>2009-10: 1.382M</p>

[△] The Government granted 2.393M at the end of 2008-09 to confirm the posts of 1 Chief Privacy Compliance Officer and 1 Senior Personal Data Officer created by the Commissioner with the PCPD's reserves.

Year of Application	Bid	Result	Year of Allocation
2009	Nil submission*		

* The Commissioner bid for funding for creation of one part in Corporate and Communications Division for promotion of awareness of PDPO and 1 temporary post for Legal Division in light of pressing need and Government advised that PCPD could consider using its reserve fund for creation of these posts.

This Work Report does not include the administrative routine of the PCPD, e.g. recruitment, personnel management, computer and system management, staff appraisal and financial management. The work detailed in this Work Report was executed by less than 29 staff.

Chapter 2: PCPD's Promotional Activities

The Ordinance provides legal protection to personal data privacy, which is the recent development of human rights legislation in Hong Kong. One of the statutory functions of the Commissioner is to promote awareness and understanding of the Ordinance among all sectors, and to ensure their compliance with the Ordinance's requirements. In order to explain to individuals (data subjects) of their rights and organizations (data users) of their obligations, the PCPD has always adopted a cost effective and problem-solving approach in organizing a wide range of activities, and to promote awareness of personal data privacy among different target groups through different medium. Below is a brief introduction of PCPD's promotional activities :

Monthly Free Introductory Seminars Held by the PCPD

The PCPD holds free introductory seminars monthly at its conference room providing members of the public with the opportunity to learn the provisions of the Ordinance and how to exercise their rights properly. The conference room holds about 50 people and almost all the introductory seminars are full.

In-house Seminars Held for Organizations

The Ordinance governs all public and private organizations in Hong Kong. To help organizations handle personal data properly, the PCPD organizes different kinds of training activities, including in-house seminars, to encourage organizations to instill the culture of personal data privacy, and teach their staff how to collect and use personal data properly. The PCPD has also designated staff to visit individual organizations to explain to their staff the Ordinance's requirements, and to provide them with practical guidance in relation to their daily operation so that they can apply what they have learnt to protect their personal data as well as those of their colleagues and clients.

Table 4 : Seminars and public forums held by PCPD between 2005 and 2009

Year	No. of In-house Seminars	No. of Participants
2005-2006	70	4616
2006-2007	49	5350
2007-2008	66	6159
2008-2009	68	5898
2009 (April to October)	36	3049

Seminars and Public Forums

From time to time the PCPD organizes seminars and public forums on different privacy topics. Local and overseas experts are invited to discuss with and advise the audience on how to protect personal data. These activities help people to become more aware of privacy issues. In the wake of a spate of online data leakage incidents that took place in 2006, the PCPD launched the "Information Security Enhancement Campaign" in collaboration with three prominent IT professional bodies. A seminar was held in 2007 which attracted more than 340 IT professionals.

Educational Activities Held for Specific Industries

"Hotel Privacy Campaign"

The PCPD has organized training courses e.g. in-house seminars to teach staff of different organizations of different sectors how to comply with the provisions of the Ordinance. To optimize the use of resources, the PCPD began to organize large-scale industry-wide educational activities in 2006 to encourage specific industry to integrate the notion of personal data privacy in their workplace. This will also raise privacy awareness among the practitioners of different levels gradually and enable them to learn good privacy practices and put them into practice.

In June 2006, the PCPD held for the first time a privacy campaign specially targeted at the hotel industry. Given Hong Kong's position as a tourism hotspot and the massive influx of tourists in the city, hotel practitioners have to

handle large amount of personal data in their daily operation. To ensure full protection of customers' data, it is necessary to raise the industry's awareness of personal data privacy in consolidating customers' confidence, and in turn anchoring Hong Kong's status as a tourism hotspot.

Apart from holding in-house seminars for each participating hotel, the PCPD had also developed an Online Self-Training Module to teach hoteliers in an easy-to-understand way how to handle personal data properly in different workplace situations. Writing competitions and self-assessment competitions were also organized to raise hotel practitioners' awareness and understanding of the privacy risks associated with their day-to-day operations. With tremendous support of the Hong Kong Hotels Association, the campaign was highly successful in that 44 hotels participated in the campaign. More than 5,000 hotel practitioners attended the 55 seminars and the message was conveyed to over 20,000 hotel practitioners.

“Personal Data Privacy Campaign for Estate Agency Trade”

The real estate sector is one of the defining factors to Hong Kong's economic development. Estate agency practitioners often collect and use customers' personal data in their daily work. Hence, it is necessary for them to comply with the Ordinance's requirements. In August 2008, the PCPD continued its efforts and held the second industry-wide privacy campaign for the estate agency trade, aimed at promoting the importance of personal data privacy and compliance with the Ordinance among real estate agents. It also encouraged employers and managers of estate agencies to implement measures to ensure that their employees comply with the Ordinance and handle customers' data properly.

The PCPD held 30 training seminars for over 1,500 estate agencies and trade associations (participants also attained CPD points under the sector's Continuing Professional Development Scheme) and took the opportunity to explain to them the provisions of the Ordinance and analyze relevant cases. A booklet entitled *Proper Handling of Customers' Personal Data by Estate Agents* was published to introduce the Ordinance and the Data Protection Principles accompanied with some case notes to help them understand the application of the Ordinance.

“Care for Patients: Protect their Personal Data” Promotional Campaign

A spate of patients’ data leakage incidents that took place in several public hospitals under the management of the Hospital Authority (“HA”) in early 2008 had aroused public concern about the protection of patients’ privacy and safety of their personal data. In May 2009, the PCPD organized a privacy campaign offering diversified educational activities to over 50,000 HA medical staff, which included seminars and online self-training modules, aimed at raising their awareness of the privacy risks in their daily work, and helping them to take precautionary measures to protect patients’ data. The one-year campaign is now underway.

Up to 31 October 2009, the PCPD had held 38 seminars for the HA and its public hospitals in that 3,740 staff members attended.

Privacy Awareness Week jointly held by Hong Kong and the Asia Pacific Privacy Authorities

It is a common goal among data protection authorities in the region to raise awareness of personal data privacy. To achieve this goal at the regional level, members of the Asia Pacific Privacy Authorities (APPA) took concerted efforts to organize an annual one-week-long promotional campaign, Privacy Awareness Week (PAW) since 2007. During the PAW, members will join hands to organize an activity, such as short video competition, writing competition, online video, etc. Moreover, individual members also hold different kinds of promotional activities on their own. Details are set out below:

Privacy Awareness Week 2007

Date	Activities
26 Aug	PAW 2007 Opening Ceremony Announcement of survey results of “Attitudes of Young People towards Disclosure of Personal Data on the Internet”
27 Aug	Seminar on “Protection of Online Personal Data” for the Data Protection Officers’ Club
29 Aug	Seminar on “Creative Thinking & Blog Writing Skills” for young people

30 Aug	Members of the Data Protection Officers' Club visited Macau Consumer Council
31 Aug	Prize Presentation Ceremony of "Privacy is Your Business" Writing Competition cum PAW Closing Ceremony

Privacy Awareness Week 2008

Date	Activities
25 Aug	PAW 2008 Inauguration Ceremony
26 Aug	Personal Data Privacy Campaign for Estate Agency Trade Kick-off Ceremony and seminar
27 Aug	Seminar for the Data Protection Officers' Club
28 Aug	"Privacy is Your Business" Video Competition Prize Presentation Ceremony
29 Aug	Public seminar for young people
30 Aug	"Privacy is Your Business" Video Competition Prize Presentation Ceremony (Macao)

Privacy Awareness Week 2009

Date	Activities
3 May	PAW 2009 Inauguration Ceremony "Privacy Reports" Launch of Privacy Awareness Week 2009 Short Animation Video
5 May	Seminar for the Data Protection Officers' Club
7 May	Launching Ceremony of "Care for patients – Protect their personal data" Campaign and seminar

Transparency of PCPD's Work

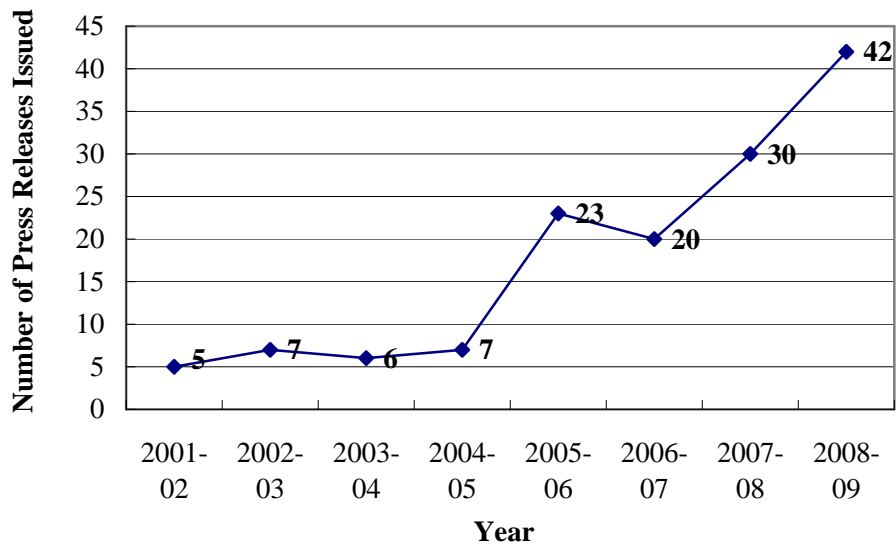
(i) Issuance of public statements

The Commissioner is committed to enhancing the PCPD's transparency by meeting the media regularly to disseminate to the public the PCPD's work progress and results.

The Commissioner is most concerned about social issues that impact on personal data privacy. The PCPD often issue public announcement to state the Privacy Commissioner's views and the application of the Ordinance in

response to any privacy related social issues so as to inform the public. For instance, the use of CCTV to monitor falling objects from a height, the installation of CCTV in taxies, the collection of clients' identification documents by lawyers for anti-terrorism and anti-money laundering purposes, online leakage of sensitive personal data, mass leakage of personal data by public and private organizations, mistaken identities of babies in hospital, drug testing in schools and so on.

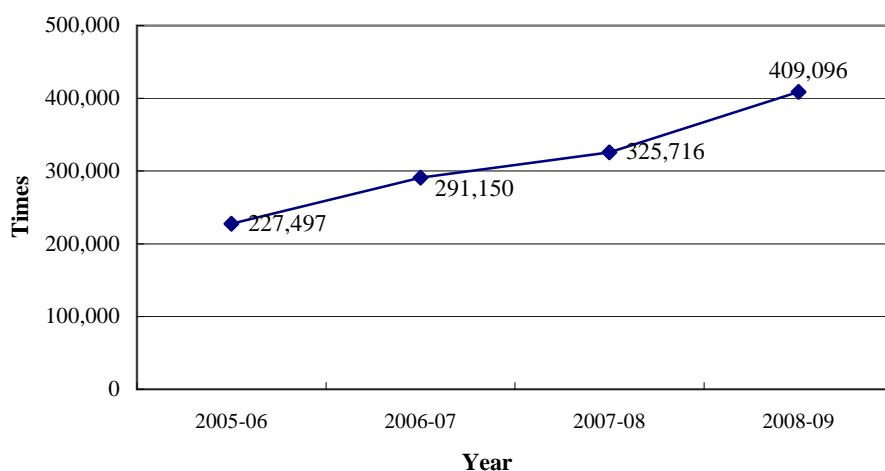
Fig. 5: Press Releases Issued by the PCPD since 2001



(ii) Busy browsing of PCPD Website

In today's Internet era, people are used to searching for information on the Internet. The PCPD therefore set up an official website in 1996 and revamped the same in 2002 to cater for the needs of the general public. The PCPD's official website, which provides abundant information and is updated from time to time, has gained popularity among the community, with the number of visitors kept increasing every year.

Fig. 6: Number of Visitors to PCPD's Website



(iii) PCPD publications

To cater for the needs of different sectors in the society for reference information in relation to personal data privacy, the PCPD has published a wide range of information materials to provide the public with its latest development and practical guidance s from different perspectives and approaches.

■ Annual Report:

- ✧ The PCPD reports its work over the year to the community in its annual report. To ensure that readers enjoy reading the annual report the Privacy Commissioner has paid special attention to make the cover design and contents of the report more attractive.
- ✧ The PCPD's annual report has won the Bronze Prize of the International Astrid Awards under the category of Annual Reports - Overall Presentation - Non-Profit – Traditional Format in 2008 and 2009. The production has won much appreciation in terms of its cover design and production quality. With entries from around the world, the Astrid Awards aims to honor outstanding achievement in design communications. Entries are judged by international panels of design professionals on the basis of concept creativity, clarity and production quality.
- ✧ Besides, the cover design of the PCPD's annual report achieved acclaimed recognition by the panel of judges in the 2009 HKMA Best

Annual Reports Awards Presentation Ceremony. According to the panel, the PCPD's annual report has clearly conveyed its policy agenda and therefore helps readers easily understand its management philosophy and ideas.

■ Newsletter :

✧ The PCPD publishes newsletters regularly providing readers with good data handling practices, PCPD's latest development and activities, overseas privacy messages as well as information about the Data Protection Officers' Club. It also elaborates the application of the Ordinance and social issues that impact on personal data privacy through case studies.

■ Guidance notes and Information leaflets :

✧ The PCPD issues from time to time guidance notes and information leaflets featuring specific social issues (such as collection of fingerprint data, property management, direct marketing, and mobile phone services). The aim is to provide data users with practical guidance in complying with the provisions of the Ordinance.

■ Booklet :

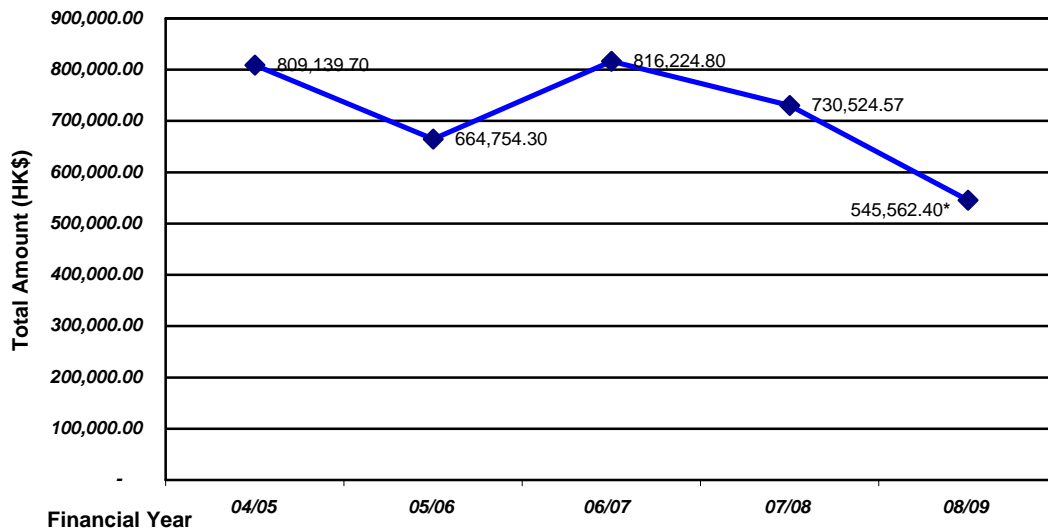
✧ By publishing booklets, the PCPD provides data subjects and data users with concise and customized information about personal data privacy protection, include *Proper Handling of Customers' Personal Data by Estate Agents, Protect Your Personal Data While Engaging in IT Related Activities, Recommended Procedures for IT Practitioners on Personal Data Handling, Respect Others and Protect Privacy*, etc.

How Much Resources are Put on Promotional Activities?

Over the last five years, the PCPD conducted the above activities on an annual fiscal budget of some \$800,000 or less (refer to **Fig. 7**). Although the promotion and publicity purposes can be better achieved through the mass media, such as advertisements, TV dramas featuring special topics, and specially produced videos, the PCPD is unable to bear the hefty costs associated with these activities. The PCPD has five staff members responsible for promotional and educational duties, whereas only one staff

member is designated to handle the training duties. Despite such difficulties in operations, staff members of the division still perform their best. Bearing the cost-effective principle in mind, they have tried their best to design and create various kinds of promotional and educational activities to disseminate the concept of personal data privacy protection to all walks of life.

Fig. 7: Promotional Expenditures for the Past 5 Years



*Excluding \$1,000,000, being one-off subsidy for the year granted on promotional projects by the Government.

Chapter 3: Educational Initiatives

One of the functions of the Commissioner is to ensure that organizations which handle personal data comply with the provisions of the Ordinance in the course of collecting, holding and using personal data. The Commissioner believes that a more far-sighted and effective means of protecting personal data privacy is to promote the concept of personal data privacy in the community and to instill the culture of respecting each other's privacy through educational activities.

Promotion to Youngsters

Youngsters are the future pillars of our society. It is therefore vital to teach them how to handle personal data with due care, especially when they are engaged in online activities.

In the past, the PCPD held various kinds of activities to attract youngsters, such as website design competitions, poster design competitions, photography competitions, writing competitions and so on. Through these activities, the PCPD provided different training courses to help them understand the importance of protecting personal data and apply their knowledge to daily life situations. For example, the PCPD held various seminars for participants in a TV advertisement competition. Apart from explaining to them the provisions and requirements of the Ordinance, the PCPD had also invited veterans from the creativity sector and the advertising sector to teach them how to produce a TV advertisement about privacy protection from the perspective of youngsters. The TV advertisements produced by these youngsters were of high standard, indicating that they truly understood the concept of personal data privacy. The participants all said that they enjoyed the learning process very much.

As for primary students of younger age, the PCPD had adopted alternative methodology of education. In 2004 and 2005, the PCPD invited a renowned youth program host to stage a musical drama entitled *Telling You My Secret* touring 50 primary schools. The show combined music, magic shows, puppet shows, games and real-life scenarios to teach the kids the proper ways of handling their personal data as well as that of their friends. The campaign

attracted over 10,000 audiences, and was made into DVDs for distribution among primary schools.

Social Opinion Survey

The PCPD attaches great importance to the general public's perspectives and expectation on personal data privacy, and has so far conducted 13 public surveys to gauge opinions from all sectors in society. Based on the results of these surveys, the PCPD was able to gain an insight into the public's attitudes towards personal data privacy and the implementation status of the Ordinance, which had been very helpful in determining the future direction of the PCPD's work.

Open Exhibitions

The PCPD takes the opportunity to react to the general public's enquiries face to face through participating in open exhibitions. For example, the PCPD takes part in Education and Careers Expo every year to remind youngsters to be cautious in providing their personal data when seeking job.

What is Data Protection Officers' Club?

The PCPD established the Data Protection Officers' Club in 2000. Target members of the club are staff members in public and private sector organizations who are responsible for handling personal data. The PCPD holds regular seminars, workshops, luncheons, visits and other activities for its members, allowing them to master the practices of personal data protection. There are currently 362 members in the Club who came from over 190 organizations. The PCPD will continue to actively recruit organizations, both big and small, to join the club so that they can learn and exchange views on the proper ways of handling personal data.

How Does PCPD Brief the Public About Cases Handled?

In order to enable all sectors to clearly understand the requirements of the Ordinance, especially the application of the data protection principles in certain circumstances, the PCPD has uploaded case notes of selected complaint cases on its official website. Over 240 case summaries are now available on the website for public information. Besides, the PCPD has prepared the summaries of the decided appeal cases heard by the Administrative Appeals Board. The purpose is to help the general public understand the opinions of the Administrative Appeals Board in relation to the Commissioner's decisions.

Reference Books Published by PCPD

To provide more detailed information to readers wishing to have a deeper understanding of the applicability of the Ordinance and how the Commissioner performs his regulatory functions in accordance with the Ordinance, the PCPD published a book entitled *Data Protection Principles in the Personal Data (Privacy) Ordinance – from the Privacy Commissioner's Perspective* in 2006, introducing in details the regulatory experience of the PCPD, the applicability of the six data protection principles and the views of the Commissioner. The book was the culmination of the joint efforts by staff members of the PCPD.

Training Tools

The PCPD has produced different kinds of training tools to meet different needs. They include:

- Online seminars
- Online self-training module (hotel sector)
- Training DVDs
- *Proper Handling of Customers' Personal Data by Estate Agents* (estate agency trade) booklet

How to Play the Role of Educator More Effectively

The educational activities mentioned above must be updated and developed in accordance with the changing environment to enable the general public to understand how technology impacts on personal data privacy, so as to optimize the functions of education. In fact, the size, format, frequency and contact area of these educational activities are subject to resources. Their progress will be hindered by external factors such as the needs to deploy resources for other contingency events. As such, the PCPD counts on a reasonable growth of resources to effectively play its role as promoter, educator and trainer.

Chapter 4: Guidance Work

In order to make clear the scope of the Ordinance to facilitate data users' compliance with relevant requirements, the Commissioner performs its guiding functions by (1) handling enquiries, (2) issuing codes of practice and guidelines, (3) conducting reviews on proposed legislations, (4) giving general advice on particular data privacy assessment projects, and (5) participating in privacy compliance audits, for the sake of providing data users with guidance. Clear guidance is useful in raising data users' understanding and awareness of personal data privacy protection, and helping them to take precautions in advance.

Enquirers are not Limited to Citizens

One of the regular duties of the PCPD is to handle the enquiries of data users and data subjects. When handling enquiries, the Commissioner will provide details about the scope of the Ordinance and the good practices of personal data protection for enquirers' reference. The PCPD staff respond to enquiries by phone, fax, e-mail and post, and sometimes at face-to-face meetings. In the year of 2008-2009, the PCPD handled 14,738 enquiry cases in total, representing a 17% increase over the previous year, and the daily handling capacity was 60 cases.

These enquiries concern is a wide variety of subjects, and the enquiries from **government departments** and **public sector organizations** are notably increasing in number. Some of these enquiries touch on the compliance with the Ordinance's requirements when carrying out projects which involve the use of personal data systems to handle massive or sensitive personal data. Besides, some **professional bodies** and parties also consult the PCPD about the applicability of the Ordinance to certain practices or acts. The handling of these enquiries are often time-consuming involving the substantial efforts of the staff. Some examples are shown below:

	Enquirer	Enquiry Case
1.	Efficiency Unit	The PCPD's opinion was sought on certain matters set forth in the draft complaint handling guidelines, including the collection and use of complainants' personal data, the storage of the data in electronic form and the management of relevant data systems.
2.	Hospital Authority	Enquired whether it is necessary to provide answers to examination questions in response to applicants' data access requests.
3.	Transport Department	The PCPD's opinion was sought on the Privacy Impact Assessment conducted in light of the establishment of a Speed Map Panel in New Territories.
4.	Constitutional and Mainland Affairs Bureau	Enquired about the personal data privacy issues in relation to the modification of e-information security policies, guidelines and regulations.
5.	Immigration Department	The PCPD's opinion was sought on the automated registration service provided to Hong Kong citizens under the Pilot Scheme on Express e-Channel launched by the Immigration Department.
6.	Transport Department	Meeting with the PCPD staff for the Journey Time Indication System (Kowloon) and enquired about the compliance with the requirements under the Ordinance for the purpose of the launch of the scheme.
7.	A law firm	The PCPD's opinion was sought on the use of consumer credit data in light of the Supervisory Policy Manual issued by the Hong Kong Monetary Authority.
8.	A professional union	Discuss how to fulfill patients' data access requests based on the requirements of the Ordinance, the administration fee associated with data retrieval, the ownership of data records, the storage/disposal of personal data records, and the impacts of using computers to handle patients' records.

	Enquirer	Enquiry Case
9.	An association	The PCPD's opinion was sought on (1) employers' collecting employees' biometric data for attendance record purpose; (2) employers' collecting employees' other personal data (such as ID card copy); and (3) the installation of CCTV
10.	A professional union	The PCPD's opinion was sought on the use of personal data of members of a particular functional constituency by the LegCo candidates of that functional constituency for communication purpose.
11.	Yau Tsim Mong District Council and Yau Tsim Mong District Office	Enquired about the installation of CCTV at Mong Kong Pedestrian Precinct to prevent falling objects from height, and the PCPD's opinion was sought on the Operation Manual of the CCTV system.
12.	Narcotics Division of Security Bureau, Education Bureau and Department of Justice	The Commissioner met with the representatives of the departments concerned to discuss the protection of students' personal data in the Trial Scheme on School Drug Testing. Opinions and seminars were subsequently provided to scheme officers.

The Issuance of Codes of Practice/Guidelines

The PCPD has issued the *Code of Practice on the Identity Card Number and Other Personal Identifiers*, *Code of Practice on Consumer Credit Data*, *Code of Practice on Human Resource Management*, and *Privacy Guidelines: Monitoring and Personal Data Privacy at Work* to address specific topics in accordance with section 12 and section 8(5) of the Ordinance. The purpose of which is to provide codes of practice and guidelines on handling ID card number and copy, consumer credit data and employment data for different data users' compliance and reference.

The PCPD has also issued guidelines on other practices or acts, such as posting recruitment advertisements, telemarketing, election, property management, collection of fingerprints and so on, with a view to preventing relevant parties from acting in breach of the requirements of the Ordinance.

Assisting the Government and Legislative Council to Formulate Various Legislations

One of the major functions of the Commissioner is to review proposed **legislations** in accordance with section 8(1)(d) of the Ordinance, advising relevant policy bureaux, government departments, and the Legislative Council on issues which may affect personal data privacy.

To perform this function, the **PCPD's Legal Division** reviews from time to time the bills published in the Government Gazette.

During the four years from 1 August 2005 to 31 July 2009, the PCPD reviewed a total of 113 bills and compiled reports on 46 of them. Please refer to **Table 8** for bills in respect of which the Legal Division issued a report and submitted opinions to the **LegCo Bills Committee**.

Table 8: Proposed Legislation Commented by the PCPD

Year 2005 (since 1 August 2005)

1. Construction Workers Registration Ordinance
2. Building Management (Amendment) Bill 2005
3. Product Eco-responsibility Bill
4. Marriage (Introduction of Civil Celebrants of Marriages and General Amendments) Bill
5. Copyright Exemption for Persons with a Print Disability
6. St. Stephen's College Incorporation (Change of Name of the Council of St. Stephen's College and General Amendments) Bill 2005
7. Carriage by Air (Amendment) Bill 2005

Year 2006

1. Construction Industry Council (No.2) Bill
2. Proposed Legislative Framework on Interception of Communications and Covert Surveillance
3. Landlord and Tenant (Consolidation) (Amendment) Bill
4. Chief Executive Election and Legislative Council Election (Miscellaneous Amendments) Bill 2006
5. Building Management (Amendment) Bill 2005
6. Interception of Communications and Surveillance Bill
7. Unsolicited Electronic Messages Bill
8. Financial Reporting Council Bill
9. Copyright (Amendment) Bill 2006
10. Implementation of Financial Action Task Force - Special Recommendation 7
11. Companies Ordinance, Financial Reporting Council Ordinance - Companies (Revision of Accounts and Reports) Regulation
12. Proposed Amendments to the Mandatory Provident Fund Schemes Ordinance
13. Race Discrimination Bill

Year 2007

1. Buildings (Amendment) Bill 2007
2. Companies (Revision of Accounts and Reports) Regulation
3. Mainland Judgments (Reciprocal Enforcement) Bill
4. First Draft of the Quarantine and Prevention of Disease (Amendment) Bill
5. Unsolicited Electronic Messages Bill
6. Energy Efficiency (Labelling of Products) Bill
7. Communications Authority Bill
8. Mandatory Provident Fund Schemes (Amendment) Bill 2007
9. Independent Police Complaints Council Bill
10. Quarantine and Prevention of Disease (Amendment) Bill 2007
11. Prevention and Control of Disease Bill
12. Product Eco-responsibility Bill

Year 2008

1. Mandatory Provident Fund Schemes (Amendment)(No.2) Bill 2007
2. Independent Police Complaints Council Bill
3. Product Eco-responsibility Bill
4. Munsang College and Heep Yunn School (Change of Corporate Names and General Amendments) Bill 2008
5. West Kowloon Cultural District Authority Bill
6. Road Traffic Legislation (Amendment) Bill 2008
7. Fixed Penalty (Smoking Offences) Bill
8. Prevention and Control of Disease Bill
9. Buildings (Amendment) Bill 2007

Year 2009 (till 31 July 2009)

1. Legal Practitioners (Amendment) Bill
2. Proposed amendments to the provisions of the Mandatory Provident Fund Schemes Ordinance
3. Proposals for allowing the public to search title register under the Land Titles Ordinance
4. Mandatory Provident Fund Schemes (Amendment) Bill 2009
5. Genetically Modified Organisms (Control of Release) Bill

Most of the opinions offered by the PCPD were accepted by the relevant bodies. One example is the Interception of Communications and Surveillance Bill, where the PCPD opined on personal data privacy issues on all fronts. The PCPD's review function is essential in ensuring that the LegCo thoroughly considers the impacts of any new legislation on personal data privacy.

Opinions Given to the Government for Public Consultation Documents

From 2005 to 2008, the PCPD submitted responses to a number of public consultation documents covering topics like **medical reform**, **copyright protection in the digital environment**, the creation of a **sex offender register** for stakeholders' reference. The Commissioner expects data users to consider and comply with the requirements of the Ordinance during the research and

development stages of any project which may impact on personal data privacy.

Opinions Given to the Government for Public Projects Having Significant Privacy Impact

The Government and public sector organizations from time to time seek opinions from the PCPD on projects which may have a profound or material impact on personal data privacy before their launch. The Private Impact Assessment conducted by the Immigration Department before the launch of the **Smart Identity Card** is a good example.

The PCPD also gives specific and comprehensive views on issues contained in reports and public consultation documents of the **Law Reform Commission** which touch on personal data privacy.

The Work of Privacy Compliance Audits

To best mitigate the risks associated with personal data privacy, it has become a norm for institutional data users to conduct regular privacy compliance audits on their personal data privacy systems. Examples include the annual compliance audit conducted by **credit reference agencies** in accordance with the requirements under the *Code of Practice on Consumer Credit Data*, and the privacy compliance audit of smart identity card data by the **Immigration Department** with the PCPD's assistance. Both examples illustrate the responsible practices of organizational data users, and their collaboration with the PCPD.

Resources and the Role of Autonomy and Independence

Given institutional data users' expectation for more comprehensive guidance from the PCPD and the complexity and variety of the technologies related to personal data systems, the PCPD has to devote more resources to optimize its functions and cater for the needs of the market and the general public. When participating in relevant initiatives, the PCPD stays independent to avoid any conflict with its regulatory functions. It is important for the Government to increase the annual funding to the PCPD so that the Commissioner can play his guiding role more effectively.

Chapter 5: Compliance Work

What are Compliance Checks?

The Commissioner believes that taking an active role in carrying out compliance actions is more important than conducting investigations in response to a complaint, since the former option is effective in preventing non-compliance in advance, especially when it comes to handling massive or sensitive personal data. Hence, the Commissioner set up the Compliance Division in December 2006 to carry out compliance checks against data users in respect of issues which raise social concerns or greatly impact on personal data privacy. The purpose of which is to sort out the problems, provide opinions and call for measures to improve certain situations. If data users refuse to take heed of the advice, the Commissioner may invoke section 38(b) of the Ordinance and take the initiative to carry out an investigation.

In many cases, data users take immediate action to correct the suspected breach. If appropriate, the Commissioner will demand from the organizations an undertaking in writing to the PCPD that they will cease the practices or acts allegedly in breach of the requirements of the Ordinance. Moreover, those institutional data users will also seek advice from the Commissioner on measures to be taken to prevent further breaches.

The Commissioner carried out 112 compliance checks in total in 2008-2009. Below are some examples:

	Institutional Data Users	Compliance Checks
1.	A few solicitors' firms	The personal data of clients of a few solicitor firms are disclosed owing to the existence of sharing software on the internet. Upon a compliance check by the PCPD, the Law Society held training courses and issued notices to highlight the significance of data security, in order to raise members' awareness of personal data security.

	Institutional Data Users	Compliance Checks
2.	A bank	<p>A bank sent monthly securities trading statements to several clients by mistake as a result of a faulty manual operation of the envelope barcode reader. Upon a compliance check by the PCPD, the bank undertook to the Commissioner in writing it would introduce an automated system to handle the delivery of letters to prevent similar incidents in the future.</p>
3.	A bank	<p>A bank had lost a server containing personal data of 50,000 clients. In May 2008, the bank informed the Commissioner one of its branches had lost a server containing 159,000 bank accounts, of which over 50,000 were bank accounts belonged to individual clients.</p> <p>According to the bank, the server was left unattended on the floor of the branch for about half an hour. Meanwhile, some workers were carrying out renovation works in the branch.</p> <p>As a remedy, the bank sent letters of apologies to all affected clients and submitted a written undertaking to the Commissioner in July 2008.</p> <p>According to the terms of the undertaking, the bank would take all practicable steps to ensure that no servers containing clients' personal data would be left unattended during the renovation of the office, and that staff members or contractors entrusted by the bank to handle clients' personal data are reliable, prudent and capable.</p>

	Institutional Data Users	Compliance Checks
4.	A developer	A developer collected identity card numbers from participants in a lucky draw activity held in its shopping malls. Upon a compliance check by the PCPD, the developer undertook to the Commissioner in writing it would cease to collect identity card numbers and destroy all identity card numbers collected.
5.	A bank	A bank overcharged clients when handling their data access requests. The PCPD then explained to the bank the requirements of the Ordinance which stipulates that no excessive fee be charged for compliance with a data access request from data subject. The bank subsequently took measures to revise downward all relevant fees.
6.	A government organization	A government organization allowed public access to personal data of applicants of its services on the internet. The government organization subsequently undertook to the Commissioner in writing it would take all practicable steps to remedy the situation in order to comply with the requirements of the Ordinance.

Investigations are not Solely Initiated by Complaints

If a suspected breach raises considerable social concerns, the Commissioner will not wait until a complaint reaches him, but will instead consider taking the initiative to carry out an investigation according to section 38(b) of the Ordinance. Moreover, if any material breach is identified during the compliance checks, the Commissioner will also initiate an investigation to decide whether or not to serve an enforcement notice on the data user directing it to correct an act or take suitable remedial measures. Below are some cases of active investigations:

	Data Users	Incidents	Investigation Results
1.	Hongkong Post	Pinhole cameras were installed at Cheung Sha Wan Post Office to detect stamp theft cases.	The Commissioner was of the view that Hongkong Post collected staff's personal data by unfair means, contravening Data Protection Principle 1(2) and had not formulated personal data privacy policy in relation to video monitoring activities, contravening Data Protection Principle 5. An Enforcement Notice was issued, directing it to cease the practice and formulate video monitoring privacy policy and implement effective measures to ensure staff's compliance.
2.	A government department	The problems associated with the computer program of the data user affected the marks of 670 candidates sitting for the English Language (Syllabus B) Examination. The incident concerned the accuracy of personal data.	The Commissioner believed that the data user was in contravention of Data Protection Principle 2(1), and therefore issued an enforcement notice to the data user directing it to take a series of measures to prevent similar incidents in the future, including formulating policies and guidelines, providing training to staff, etc.
3.	A primary school	A primary school collected fingerprints from students and teaching staff for attendance purpose. The incident involved collecting excessive personal data.	The Commissioner believed that the primary school was in contravention of Data Protection Principle 1, and therefore issued an enforcement notice directing it to cease collecting fingerprint data and destroy all fingerprint data collected.

	Data Users	Incidents	Investigation Results
4.	A recruitment agency	A computer file containing personal data of about 39,000 job applicants was found freely accessible and downloadable by the public via the internet. The personal data were held by the recruitment agency. The incident involved the security of personal data.	The recruitment agency undertook to the PCPD in writing that it would take all measures reasonably practicable to ensure the safety of the personal data it collected and prevent similar incidents in the future. The Commissioner considered that the recruitment agency was in contravention of Data Protection Principle 4, and therefore issued a written warning to it.
5.	A credit agency	A credit agency sent letters to the public inviting them to provide personal information including identity card number and the name of their employers in exchange for a supermarket coupon worth HK\$20 for promotional purpose. The incident involved collecting excessive personal data.	Upon the launch of an investigation, the credit agency deleted the identity card numbers and names of employers collected during the promotional activity, and ceased to collect identity card numbers, other personal identifiers and employers' names in similar promotional activities. The Commissioner considered that the credit agency had collected excessive personal data in the incident and was in contravention of Data Protection Principle 1(1) and the requirements under paragraph 2.3 of the Code of Practice on the Identity Card Number & Other Personal Identifiers.

	Data Users	Incidents	Investigation Results
6.	Independent Police Complaints Council (“IPCC”)	The online leakage of personal data of some 20,000 people who had filed complaints against the Police was put on the internet for public access and download. The incident involved the security of personal data.	The Commissioner served an enforcement notice on IPCC directing it to formulate policies and guidelines for regulating the practices of handling personal data among outsourced contractors or agencies, implement effective measures to ensure its staff’s compliance with such policies and guidelines; and review contracting agreement to stipulate therein the measures required to be taken by contractors for the sake of protecting the personal data provided to them by IPCC.

What is a Matching Procedures Application and How is it Handled by PCPD?

Part VI of the Ordinance regulates the matching procedures for personal data. The “matching procedures” refer to the use of non-manual ways to compare two sets of personal data collected from at least ten data subjects for different purposes, and take action against relevant data subjects in case of a successful matching between the two sets of data.

The matching of data will affect personal data privacy as the matching practice may not be consistent with the original purpose of data collection, and it may contravene the requirements under Data Protection Principle 3 unless the prescribed consent of the data subject was obtained. As such, data users wishing to carry out the “matching procedures” must fulfill the requirements of the Ordinance. Save for exceptional situations, no matching procedures will be allowed without the prior approval of the Commissioner. Most of these applications are originated from Government departments / bureaux or statutory bodies.

According to the requirements under section 32 of the Ordinance, the Commissioner may approve data users to carry out data matching lawfully. Other factors to be considered by the Commissioner include whether or not the matching procedures are in line with the public interest and whether there is any practicable alternative.

The Commissioner received altogether 29 applications for carrying out matching procedures in 2008-2009. Below are some examples:

	Requesting Parties	Matching Procedures Approved
1.	Home Affairs Department	Consent was given to Home Affairs Department to carry out a matching procedure to ensure the accuracy of the voter registers for the Village Representative Election ("VRE") by comparing personal data collected by Home Affairs Department for the purpose of VRE with personal data maintained by the Registration of Persons database of Immigration Department.

	Requesting Parties	Matching Procedures Approved
2.	Hong Kong Housing Society	Consent was given to Hong Kong Housing Society to carry out a matching procedure to prevent double housing benefits by comparing personal data collected from applicants for the Building Maintenance Grant Scheme for Elderly Owners with personal data collected by Buildings Department from applicants for the Building Safety Loan Scheme.
3.	Social Welfare Department	Consent was given to Social Welfare Department to carry out a matching procedure to prevent double subsidies by comparing personal data collected by Social Welfare Department from recipients of the Comprehensive Social Security Assistance with personal data collected by Labour Department from recipients of transport subsidies under the Transport Support Scheme.
4.	Social Welfare Department	Consent was given to Social Welfare Department to carry out a matching procedure to prevent fraud or abuse of social security benefits in relation to retraining allowance by comparing personal data collected from recipients of the Comprehensive Social Security Assistance with personal data collected by Labour Department for administering the retraining allowance under the Manpower Development Plan for the textiles and clothing industry.
5.	Fire Services Department	Consent was given to Fire Services Department to carry out a matching procedure to detect double housing benefits by comparing personal data of departmental quarters applicants held by Fire Services Department with personal data of public housing estate tenants and owners maintained by Housing Department.

	Requesting Parties	Matching Procedures Approved
6.	Official Receiver's Office	Consent was given to Official Receiver's Office to carry out a matching procedure to identify bankrupts who have left Hong Kong without complying with the requirements of the Bankruptcy Ordinance by comparing personal data collected by Official Receiver's Office for administering the Bankruptcy Ordinance with the personal data collected by Immigration Department for immigration clearance.
7.	Mandatory Provident Fund Schemes Authority	Consent was given to Mandatory Provident Fund Schemes Authority to carry out a matching procedure to ensure certain members are eligible for receiving the special contribution of \$6,000 by comparing personal data of members of MPF scheme and ORSO scheme with personal data of members of similar schemes administered by Treasury and Education Bureau.
8.	Education Bureau	Consent was given to Education Bureau to carry out a matching procedure to prevent double subsidies by comparing personal data collected by Education Bureau from applicants of the Pre-primary Education Voucher Scheme with personal data collected by Social Welfare Department from recipients of the Comprehensive Social Security Assistance and recipients under the Child Care Centre Fee Assistance Scheme.
9.	Student Financial Assistance Agency	Consent was given to Student Financial Assistance Agency to carry out a one-time matching procedure to prevent double grants of one-off new school term allowance by comparing personal data of student recipients in the 2008/09 academic year with personal data collected by Social Welfare Department from student recipients of the Comprehensive Social Security Assistance.

	Requesting Parties	Matching Procedures Approved
10.	Registration and Electoral Office	Consent was given to Registration and Electoral Office to carry out a matching procedure to identify electors of the geographical constituencies who have moved out and may become ineligible to vote in their original constituencies by comparing personal data collected by Registration and Electoral Office for the purpose of District Council Elections and Legislative Council Elections and their by-elections with personal data collected by Home Affairs Department for the purpose of Village Representative Elections.

The Unprecedented Inspection over Personal Data System

The Commissioner is empowered under section 36 of the Ordinance to carry out an inspection over any personal data system maintained by data users and make recommendations accordingly. In the light of a series of patients' data leakage incidents in early 2008, the Commissioner exercised the power for the first time on 8 May 2008 to inspect Hospital Authority's patients' data system to promote the Hospital Authority's compliance with the Ordinance. The inspection and recommendation focused on the security of patients' data systems. In this exercise, the Commissioner not only deployed the PCPD staff, but had also solicited assistance from four consultants in the privacy, legal, medical and IT fields. The inspection work included:

- ◆ an examination of Hospital Authority's relevant policies, manuals and guidelines in relation to patients' data protection;
- ◆ face-to-face interviews with responsible personnel of head office of the Hospital Authority and hospitals under it;
- ◆ face-to-face interviews with some 100 randomly selected staff for completing the questionnaire specially designed for the inspection and an assessment of the returned questionnaires; and
- ◆ the walk through of various departments of hospitals to examine the actual operation.

In this inspection, the Commissioner deployed more than half of the PCPD staff and published a report on the inspection over Hospital Authority's personal data system on 22 July 2008, in which he put forward 37 recommendations to the Hospital Authority to address relevant problems. Examples include:

- ◆ There should be systematic formulation, review and updating of data security policies and practices and their effective dissemination to the Hospital Authority staff;
- ◆ The functional roles to be played by the Hospital Authority's Cluster Committees should be clearly defined and that of the Data Controller should be strengthened to protect patients' data security;
- ◆ The security measures adopted by Hospital Authority should be strengthened to reduce the risk of unauthorized or accidental access to patients' data;
- ◆ Hospital Authority should develop systematic data security audit methodology to be followed by all hospitals;
- ◆ To tighten supervision of compliance and give more education and training to the staff;
- ◆ To make it a policy to conduct privacy impact assessment; and
- ◆ To give data breach notification upon happening of a data security breach.

Before 2008/2009, Government did not allocate resources to PCPD for conducting inspection. Ever since the Commissioner's strenuous efforts in utilizing own resources to conduct this inspection exercise, Government approved the granting of some fund in future for the conduct of inspection by the Commissioner for one or two times a year.

How PCPD Handles Complaints Received?

The "Selective to be Effective" Approach

Given the limited resources of the PCPD, it is impossible to carry out thorough investigation on every single complaint. Thus, it is necessary to have a mechanism in place to select appropriate cases for investigations and enforcement action. The Commissioner is vested with the discretion by the Ordinance not to initiate or discontinue an investigation after taking into

account all the circumstances of the case. The PCPD has formulated the Complaint Handling Policy for this purpose.

Unsubstantiated

Upon receipt of a complaint, the PCPD's case officers will carry out preliminary inquiry and contact the complainant and obtain supporting data related to the case, and explain to the complainant relevant requirements under the Ordinance. The data collected will be studied and, if the case does not fall within the jurisdiction of the Commissioner (such as not involving "personal data") or does not establish a prima facie case, the PCPD will notify the complainant in writing explaining its decision of not commencing an investigation and the reasons behind.

Mediation

In some cases, the PCPD's case officers will conduct mediation and explain to the data users concerned the Ordinance's requirements, and request them to take remedial measures, though there is no such requirement under the Ordinance. Under the circumstances where the complainant is satisfied with the result, or the Commissioner believes that no better result can be achieved by a thorough investigation, the case will be closed. In this case, the PCPD will notify the complainant in writing of its decision of closing the case and the reasons behind. The PCPD will also provide advice or recommendations to the data users.

Investigation

In case of a serious complaint (e.g. loss of patients' data by United Christian Hospital, leakage of complainants' data by Independent Police Complaints Council, etc.), or an unsuccessful mediation (e.g. complainees refused to take remedial action according to the PCPD's recommendations), the PCPD will then carry out a formal investigation. The PCPD believes that the complaint mechanism set up by the Ordinance is to improve the personal data handling policies and practices of data users, and does not aim at punishment. Therefore, when there is any contravention, the PCPD will generally handle the complaints by means of education, mediation and urging the data user concerned to improve its practice in handling personal data, so that the

protection of personal data privacy in the society can be enhanced on the whole. In view of the above factor and the effective use of limited resources, the PCPD will only carry out formal investigation on complaint cases which are supported by sufficient prima facie evidence, serious in nature, cannot be resolved by mediation and/or in which the complainee refused to improve its practice. Therefore, the number of investigations carried out by the PCPD in the past is not high.

During investigation, case officers will collect information and evidence from the complainant and complainee; if necessary they and related third parties may be invited to the PCPD to give statements. When there is inconsistency between the data provided by the complainant and complainee, e.g. the complainant claimed that his employer (complainee) had not issued any written internal code or guideline, but the complainee denied, apart from asking both parties to provide supporting documents, the PCPD will invite other employees of the complainee to provide information as witnesses so as to help the PCPD understand more about the case.

However, the PCPD may not be able to obtain information and evidence smoothly in every cases. In the past, the PCPD had come across uncooperative complainee and/or other party concerned. They did not respond or fully respond to the PCPD's written enquiries and the case officers could not contact them by phone. Under such circumstances, the PCPD has to issue a summons under the Ordinance requesting them to attend the PCPD's inquiry and provide relevant data documents.

Moreover, if a case is related to the personal data system of the complainee, or the PCPD has to verify the saying of the complainee (e.g. the complainee said that the circular involved had been renewed), the PCPD's case officer may need to pay on-site visit to verify the actual situation. If the on-site investigation is to be carried out at the complainee's premises, the Commissioner has to notify the complainee before the on-site investigation, of the time and premises where he will exercise such power under the Ordinance.

For cases which may involve the operating mode/practice of the entire sector, the PCPD will also make enquiries to the regulatory organization to which the data users belong, or seek opinions from the association/society to which the data users belong to assist investigation.

If the nature of a case is complicated, and/or important legal issue is involved, the PCPD will have thorough and detailed discussion on it before making a decision. Counsel of the Legal Division will also assist in case analysis and provide legal advice.

It can be seen that before completion of an investigation, the PCPD needs to take different actions according to the specific situation of each case. Other practical difficulties that the PCPD may encounter in handling complaint cases can be found under “The Role of and Problems Facing the PCPD” below. The resource constraint means that the Commissioner needs longer time to finish an investigation.

Decision of Not Carrying Out or Continuing an Investigation

If the PCPD decides not to carry out or continue an investigation, the Commissioner is required under the law to notify the parties concerned in writing of the decision and the reasons. The complainant may appeal to the **Administrative Appeals Board** against the PCPD’s decision of not carrying out an investigation. Therefore, the decisions made by the PCPD must be lawful, just and reasonable. When informing the complainant in writing of the reasons for the decision of not carrying out an investigation, the PCPD has to explain its reasoning in detail and carefully to the complainant and the party concerned who has the right to lodge an appeal under the Ordinance.

After Comprehensive Investigation: Enforcement Notice and Criminal Crimes

Upon completion of a formal investigation, should the Commissioner consider that the data user complained against is breaching or has breached the Ordinance’s requirements, and the breach is likely to sustain or recur, the Commissioner may serve an enforcement notice on the data user directing it to take remedial measures. The PCPD has to confirm if the data user has complied with the requirements of the enforcement notice. It is an offence if the data user fails to comply with the enforcement notice, in which case the PCPD will refer the case to the Police for prosecution.

Serving Enforcement Notice or Not?

No matter whether the Commissioner has served any enforcement notice in a case, the complainant and the data user can appeal to the Administrative Appeals Board as provided under the Ordinance. Therefore, when informing the complainant and complaine in writing of the investigation result, the PCPD has to be more careful and comprehensive in detailing the causes and consequences of the case so as to let the complainant and complaine understand the reasoning. This is also an important basis for appeal hearing.

Issuing Reports for Public Interest

Apart from preparing a detailed investigation result and delivering the same to the complainant and the complaine, 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 an open report setting out the result of the investigation as well as any recommendations or comments. If the investigation results involve issues of public concern, and have significant impact on or harm to personal data privacy, e.g. application of technology on the use and security of personal data, the Commissioner will consider issuing a report to strengthen the public's knowledge and privacy awareness. The Commissioner has so far published ten investigation reports and an inspection report (see **Table 9**), which were issued during the tenure of the Commissioner except the one report issued in 1997. They included investigations of IPCC **online data leakage** incident, **loss of patients' personal data** by hospitals, and employers' **collecting employees' fingerprint data** for attendance purpose, etc.

Table 9: 11 Investigation and Inspection Reports published by the Commissioner

Issued Date	Investigation Reports
1. 13 October 1997	Unfair collection of personal data by covert video tapping in hostel room of a university and disclosure of personal data so collected
2. 8 December 2005	The practice of collection of employees' personal data by pinhole cameras without proper justification was excessive and unfair in the circumstances of the case
3. 26 October 2006	The security measures to be taken by an outsourced contractor in protecting personal data entrusted to it

Issued Date	Investigation Reports
4. 14 March 2007	The disclosure of email subscriber's personal data by email service provider to PRC law enforcement agency
5. 21 September 2007	Collection of personal data by credit provider for business promotion
6. 24 December 2008	Loss of patient's personal data by United Christian Hospital
7. 19 January 2009	University refusing to comply with data access request in relation to examination marking
8. 13 July 2009	Employer collecting employees' fingerprint data for attendance purpose
9. 3 August 2009	A tutorial centre using a student's results notice for promotion without the student's consent
10. 7 August 2009	Food company collecting participants' personal data in lucky draw activity

Issued Date	Inspection Report
1. 22 July 2008	Report on the inspection of the Hospital Authority's patients' data system

Unlike the case notes published on the PCPD's website, these reports contain every detail of the investigation result and the recommendations put forward by the Commissioner, and provide people from all walks of life with more in-depth and comprehensive coverage of the reasons and bases behind the Commissioner's decision on a particular case for their reference. Coupled with the release of a report, the Commissioner will issue a press release or hold a press conference to answer enquiries from the media.

The Role of and Problems Facing the PCPD

The duties to be carried out by the PCPD when handling complaints include exercising its function to **regulate, advise, mediate, investigate, rule and enforce**, etc. Both the complainant and the complainees may appeal against the investigation result of the PCPD. Some complainants and complainees have instead chosen to file a complaint against the PCPD's decision with other organizations, such as the Chief Executive's Office, Ombudsman, and the

Constitutional and Mainland Affairs Bureau, or bring the cases to the court. The PCPD has to respond to all these one by one. Hence, the PCPD always carries out its work with caution and prudence. The following are the problems frequently encountered by the PCPD when handling complaints:

(i) Complexity and difficulty of the complaint cases

The PCPD must handle each complaint with due care. Although the number of complaints has slightly decreased in recent years, their complexity has been increasing and the number of cases soars again recently (see **Fig. 10**). The problems encountered by the PCPD have increased. Besides observing the Ordinance's requirement that the Commissioner must notify the complainant in writing of his decision not to carry out or discontinue the investigation and the reasons within 45 days from the date of receipt of the complaint, such cases have become more complex and difficult to handle. For instance, the PCPD once received a complaint which required the case officers to review a supporting document – a tape containing recorded information which lasted for some 65 hours. Besides, since the occurrence of the Lehman Brothers incident, the PCPD has received many complaints concerning banks' refusal to handle clients' data access requests, and such complaints involve a great deal of recorded telephone conversations and relevant transcripts. The case officers have to spend much effort and time on these kinds of complaints. In addition, the appeal case in relation to the disclosure of email account holders' data by Yahoo Hong Kong Limited to PRC public security authorities (which allegedly led to a 10 years' imprisonment of a mainland reporter) and the Cathay Pacific Airways Limited's collecting the medical records from its cabin crews show that many complaint cases handled by the PCPD are of a high degree of complexity and difficulty.

(ii) Higher public expectation on PCPD's complaint handling: thorough investigation and better services

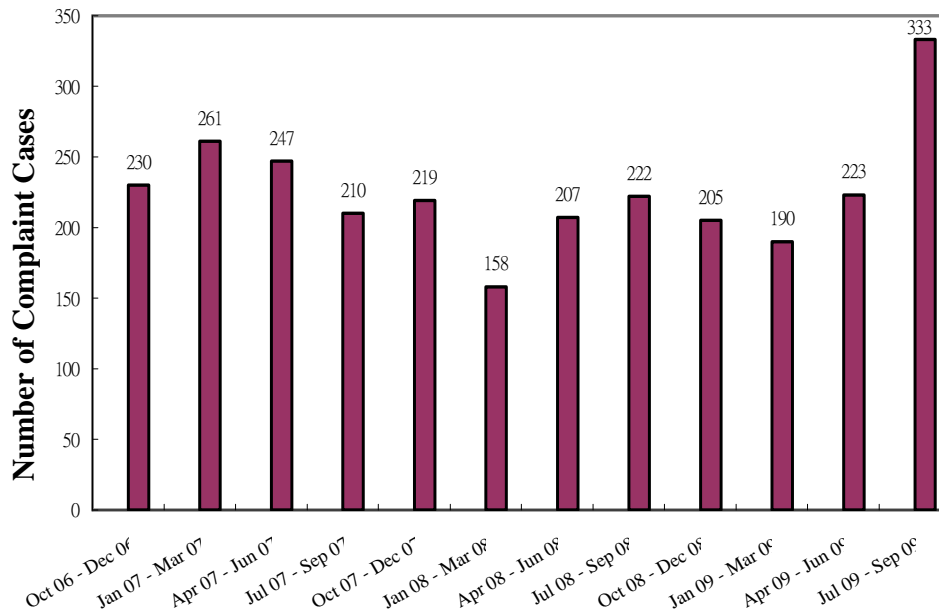
As the public awareness of personal data privacy is higher than 10 years ago and expectation of different sectors on the regulatory role of the PCPD is increasing, the PCPD needs to handle the cases with care and prudence. For instance, although the PCPD has learnt from the complainant that the company complained against was closed, the PCPD's case officer will still carry out company search and on-site observation to confirm the closure of the company.

Moreover, the PCPD will still send an enquiry letter to the company and wait until the response deadline expires. If no reply is received, the PCPD can then decide not to carry out an investigation. In a complaint received by the PCPD, the complainant initially complained against a company of unfair collection of his/her personal data. After listening to the recorded telephone conversation, the PCPD's case officer found that the allegation of the complainant was not substantiated. When the case officer informed the complainant of the information obtained and the decision made, the complainant then complained another organization which disclosed his/her personal data to the company. As such, the PCPD had to continue handling the case. This example can explain why the time of handling complaints is longer than before. Fig. 10 illustrates an obvious increasing trend of complaint cases in the first nine months of 2009. The complaint officers are experiencing an increased workload.

(iii) Staff re-deployment and high turnover rate

The high turnover rate of complaint handling officers in the Operations Division (33% in 2004 to 67% in 2008), the decrease in the number of senior staff (10 Personal Data Officer in 2004, but only 4 Personal Data Officer and 4 Assistant Personal Data Officer in November 2009), and deployment of staff to handle additional projects (e.g. inspection of Hospital Authority and Ordinance Review exercise) have inevitably put an additional strain on PCPD's resources and thus affected the pace at which these complaint cases are handled.

Fig. 10: Complaint Cases Received by the PCPD on a Quarterly Basis between October 2006 and September 2009



How Does PCPD’s Operations Division Operate Under Limited Resources?

The Operations Division charged with handling complaints has maintained a team of about 10 staff members over the years. The work nature of handling complaints, complexity of cases and inability to forecast the number of new complaints are reasons for high staff turnover. Staff turnover and re-deployment of staff for work needs (see **Table 11**) have exerted work pressure on staff and this also accounts for the building up of backlog of cases.

Table 11: Turnover Rates of Complaint Handling Officers in Operations Division from 2004 to 2008

Year	Officers Departed/ Transferred Out	Turnover Rates
2004	4	33% (4/12 x 100%)
2005	4	31% (4/13 x 100%)
2006	7	50% (7/14 x 100%)
2007	4	29% (4/14 x 100%)
2008	8	67% (8/12 x 100%)

With the principle of effective use of resources in mind, the Commissioner, while performing his functions, must consider whether the incident has considerable effects on personal data privacy, the harm caused to data subjects, and whether it involves considerable public interest. Such practices have been made known to the public through the Complaint Handling Policy issued by the PCPD. The Commissioner also prefers negotiations, explanations, and improvement measures initiated by data users such as signing a written undertaking to prevent similar breaches and make prompt and effective mediation, instead of exercising investigation power on every complaint case to enforce the compliance with the Ordinance's requirements. For suspected contravention which has serious impact on personal data privacy or involves serious public interest, the Commissioner will consider taking the initiative to investigate and follow up even if there is no complaint.

Chapter 6: Enforcement Work

PCPD's Referral of Cases to the Police for Prosecution

According to the Ordinance, it is an offence if a data user contravenes a provision or requirement of the Ordinance. Since the Commissioner has no power of prosecution, he can only refer a case to the Police for possible prosecution after he has taken into account the specific circumstances of the case, including whether there is enough prima facie evidence, the seriousness of the case, whether the complainant is willing to attend court as a witness and whether the data user has previously been complained for similar reasons.

Before referring a case to the Police, the case officer needs to take depositions from relevant data subjects, obtain supporting data from other relevant witnesses, and seek legal advice whenever necessary. Since the time bar for prosecution of a case falls within 6 months from the date the case occurs, the case officer should collect relevant data swiftly so that the Police will have sufficient time to carry out investigations and take prosecution action.

The PCPD previously referred certain cases to the Police for prosecution against the data users who were suspected to have breached the Ordinance's requirements as set out below:

- 1) Section 19 of the Ordinance - mainly concerns the data users' non-compliance with data subjects' data access requests within the 40-day period;
- 2) Section 34 of the Ordinance - mainly concerns the data users' non-compliance with "opt-out" requests from data subjects;
- 3) Section 64(7) of the Ordinance - mainly concerns the data users' non-compliance with the directions specified in the enforcement notices issued by the PCPD in accordance with section 50 of the Ordinance; and
- 4) Section 64(9) of the Ordinance - mainly concerns the making of false statements to the PCPD during the PCPD's investigation.

From 1998 to 30 September 2009, the PCPD has altogether referred 42 cases involving suspected breaches of the Ordinance to the Police for follow-up actions, among which there are nine cases where the parties concerned have been charged and convicted in a magistrate's court. The nine cases can be classified by their nature as follows: five cases concern the data users' non-compliance with data subjects' "opt-out" requests; three cases concern data users' non-compliance with the directions set forth in the "enforcement notices" issued by the PCPD in accordance with the Ordinance, and one case touches on the data user's non-compliance with the data subject's data access request. Offenders are generally imposed a fine of several thousand dollars by the court.

Problems Encountered by PCPD in Handling Administrative Appeals and PCPD's Performance

There is a mechanism in place under the existing Ordinance allowing those who are not satisfied with the Commissioner's decisions on complaint cases to appeal to the Administrative Appeals Board. During the entire appeal proceedings, the PCPD's Legal Division is responsible for all defence works in relation to the appeals against the Commissioner's decisions, including the preparation of a statement of defence, disclosure of documents, preparation of written statements, making oral submission during a hearing, responding to all relevant questions, etc.

During the four years from 1 August 2005 to 31 July 2009, the PCPD's Legal Division handled 104 administrative appeal cases in total. The number of administrative appeal cases had been increasing every year, until it hit the record high of 28 cases in 2007. Although the number of appeal cases slightly decreased to 22 in 2008, a total of 26 cases were received as of September 2009, meaning it is very likely to break the historical record of 28 cases in 2007.

Since the implementation of the Ordinance up to 30 September 2009, the Administrative Appeals Board heard and reached verdicts on 163 appeal cases, of them 146 appeals were dismissed, revoked or withdrawn, representing about 90% of all appeal cases. Such high percentage of successful defence not only demonstrates the hard work put by the Legal Division, but also the prudent

handling of complaints by the PCPD's investigation team, which allow the Commissioner to continuously make reasonable and fair decisions.

The Commissioner Can Prosecute or Be Prosecuted: Court Cases

The Commissioner is also required to handle court cases involving the PCPD. One of the examples is the widely publicized judicial review application filed by Cathay Pacific Airways Limited (hereinafter "Cathay Pacific") against the Commissioner's decision. Another example involves a case where the complainee was not satisfied with the enforcement notice issued to him by the Commissioner, and therefore initiated a civil action in the High Court and claiming damages against the Commissioner. In consideration of the complainant's failure to disclose a reasonable cause of action and his abuse of the judicial proceedings, the Commissioner applied to the court to strike out the complainant's pleadings on the grounds of, among others, the complainant's failure to disclose any reasonable cause of action, and for the sake of avoiding the hefty litigation costs resulting from the prolonged proceedings. An order was subsequently granted by the Master of the High Court to strike out the pleadings. The complainant was not satisfied with the ruling and filed an appeal with the Court of First Instance of the High Court and the Court of Appeal respectively, but the appeals were both dismissed.

PCPD's Efforts in Controlling the Costs in Handling Appeals and Litigations

When dealing with litigations and supervising litigations handled by external solicitors, the PCPD usually adopts a pragmatic approach to avoid dwelling on unnecessary points of dispute and unnecessary interlocutory applications to control litigation costs. If the matter under dispute can be settled in a practical way, without prejudicing the protection provided by the Ordinance, the Commissioner stands ready to reconcile with the other party to avoid unnecessary litigation proceedings and costs. Such a practice is clearly seen from the settlement in the Cathay Pacific case.

With the cost-saving principle in mind, the PCPD seldom engages external solicitors or barristers when handling administrative appeal cases. Even if the

appellant engaged a large team of lawyers, including solicitors, barristers and senior counsel in a recent administrative appeal, the PCPD only assigned its solicitors from the Legal Division to appear before the appeal board.

In case of an actual need to engage private practising solicitors, the PCPD has a comprehensive and stringent mechanism in place to monitor and review the legal costs associated with engaging private practising solicitors. The Commissioner and the Legal Division will strive to adopt effective measures to reduce litigation costs. Thanks to the hard work of the Commissioner and the Legal Division in the past, the PCPD managed to save substantial litigation costs in many cases. One example is the “Yahoo” appeal case, which involved complicated legal disputes which required senior counsel to handle. Although a senior counsel was retained to handle the appeal case, the PCPD was offered a low service charge. Moreover, in several civil and criminal proceedings, the PCPD successfully negotiated much lower legal service fees than the market rate.

Chapter 7: Law Reform

Background

The Ordinance came into effect 13 years ago. With the rise of the electronic era, the rapid development in technology as well as electronic trade and commerce has raised worldwide concerns over personal data privacy. In order to properly respond to the impacts of technological advancement on personal data privacy, there is a global trend to call for more comprehensive protection of personal data privacy and more stringent sanctions and laws. In this connection, Australia, Canada, New Zealand and the United Kingdom all embark actively on the review of their laws.

Personal data privacy has been an evolving concept in human rights and electronic trade and commerce in tandem with the rapid changes and development of our society. The Commissioner acknowledges the core value of balancing the personal data privacy right with public interest in maintaining a harmonious society. As a governing body, the PCPD has extensive regulatory experience in applying the Ordinance, from which the PCPD believes that the Ordinance still has much room for reform.

In June 2006, the Commissioner made an unprecedented decision to set up an internal Ordinance Review Working Group to comprehensively assess the adequacy of the protection rendered to personal data privacy by the Ordinance. In overseas jurisdictions, the work is generally handled by local law reform commissions.

Led by the Commissioner, the Working Group comprises such members as the Deputy Privacy Commissioner for Personal Data, the Chief Legal Counsel and the Chief Personal Data Officer. Upon its establishment, the Working Group underwent a series of work, including a review on previous judgments made by the court and the Administrative Appeals Board on the application and interpretation of the Ordinance, and an extensive study of the laws of personal data privacy protection and their development in overseas countries, with an aim to proposing amendments to the Ordinance. The Working Group also maintained close ties with the Government and responded to questions raised

by government departments and policy bureaux on its proposals. The Working Group has held more than 30 working meetings thus far.

Key Points of Ordinance Review

The Working Group took into account the following factors in the course of the review:

- (a) the sufficiency of protection and the proportionality of penal sanction under the Ordinance;
- (b) the development of international privacy laws and standards since the operation of the Ordinance;
- (c) the regulatory experience of the Commissioner gained in the course of discharging its functions and powers;
- (d) the difficulties encountered in the application of certain provisions of the Ordinance;
- (e) the technological development in an electronic information age facilitating the collection, holding and processing of personal data in massive quantum at a low cost;
- (f) the development of biometric technology for the identification of an individual poses challenges to the maintenance of individuals' privacy; and
- (g) the vulnerability of individuals in becoming less able to control and determine the collection, use and security of his personal data stored and transmitted through electronic means.

The Working Group had five missions to achieve in undertaking the review exercise. They were:

- **To address issues of public concern.**
- **To safeguard personal data privacy rights while protecting public interest.**
- **To enhance the efficacy of regulation under the Ordinance.**
- **To harness matters that will have significant privacy impact.**
- **To deal with technical and necessary amendments.**

After a year and a half's work, the PCPD presented to the Constitutional and Mainland Affairs Bureau a comprehensive set of over 50 amendment proposals and issues of privacy concern in December 2007. Since then, more than a year and a half was spent on discussing the proposals with the Constitutional and Mainland Affairs Bureau and holding meetings with the representatives of certain government departments.

On 28 August 2009, the Government released the **Consultation Document on Review of the Personal Data (Privacy) Ordinance** (hereinafter called "the Consultation Document"), in which 43 amendment proposals were set out for public consultation.

Amendments Proposed by the Commissioner

The amendments proposed by the Commissioner to the Government cover a wide range of topics, including:-

- (a) sensitive personal data;
- (b) data security;
- (c) enforcement powers of the Commissioner;
- (d) offences and sanctions;
- (e) rights of data subjects;
- (f) rights and obligations of data users;
- (g) introducing new exemptions; and
- (h) clarifying the scope of coverage of the Ordinance and other operational issues.

Below are some proposals which have aroused much controversies and have far-reaching impacts on personal data privacy protection.

Creating New Criminal Offences

In recent years, a series of incidents involving leakage or loss of sensitive personal data has caused grave privacy concern, for instance, the Independent Police Complaints Council's leakage of complainants' personal data, on-line dissemination of nude photos and the loss of patients' data by the Hospital Authority. While there are at present provisions under the Ordinance

regulating data users in safeguarding data security, the PCPD is of the view that it is timely to strengthen the provisions of the Ordinance to enhance the protection of personal data privacy.

In order to curb irresponsible dissemination of leaked data, the PCPD proposed to make it an offence for any person who **knowingly or recklessly**, without the consent of the data user, **obtains or discloses** personal data held by the data user or procure such disclosure unless there is reasonable justification. The PCPD also proposed to make it illegal for anyone to sell the personal data so obtained for profits.

Obligation of Outsourced Agents and Contractors

In relation to the transfer of personal data to an outsourced agent or contractor for handling, the PCPD proposed to impose an obligation on data users who engage data processing agents to use contractual or other means to ensure that the data processors and any sub-contractor will take all steps practically feasible to provide a comparable level of protection for the data and maintain them properly, and that the data will not be used by improper users and will be deleted once they are no longer needed. The PCPD further proposed that **data processing agents** should be obliged to observe certain requirements under the Ordinance, including Data Protection Principle 2(2) (duration of data retention), Data Protection Principle 3 (use of personal data) and Data Protection Principle 4 (security of personal data).

Mandatory Data Breach Notification

To mitigate or reduce the damage that may be caused to data subjects whose personal data are leaked or lost, the PCPD suggested that the Administration should consider making **privacy breach notification mandatory** so as to require data users to promptly notify individuals who are affected by the loss or theft of personal data in certain breaches where there is a real risk of significant harm. The PCPD should also be notified of the relevant events when such events happened.

Classification of Sensitive Data

The Ordinance as it presently stands does not differentiate personal data that are sensitive from those that are not. However, certain kinds of personal data are by their inherent nature commonly taken as more sensitive. Given improper handling of such data may cause significant harm to the data subjects, the PCPD proposed to amend the Ordinance to specially bring the protection level of **sensitive personal data** at par with the standard stipulated in the EU Directive 95/46/EC on *Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data*. The PCPD suggested that the new definition of “sensitive personal data” could include the racial or ethnic origin of the data subject, his political affiliation, his religious beliefs and affiliations, membership of any trade union, his physical or mental health or condition, his biometric data or his sexual life. Generally, the data subject’s consent should be obtained before collecting such data. In anticipation of the eventual implementation of electronic patient records by the Government, where massive sensitive health records are kept in databases for use and access, the PCPD considers that more stringent controls and prudent practices are required for physical and mental health data.

Review of Direct Marketing Practices

The commercial value of **direct marketing activities** is well known. However, the flourishing of such activities sometimes result in unwelcome calls and cause nuisance to the recipients. The regulatory regime under section 34 of the Ordinance is to require the direct marketers to give an “opt-out” choice to the data subject when first using his personal data for such purpose. Repeated direct marketing activities to a person who has “opted out” from such activities constitutes a breach of the provision of the Ordinance which amounts to an offence. In reviewing the effectiveness of the Ordinance in tackling the problem, the PCPD called on the Government to consult the public on whether an “opt-in” instead of an “opt-out” regime is more appropriate; whether a territorial-wide do-not-call central register should be established and whether a data user shall be required to disclose the source of the recipient’s personal data upon the latter’s request. The penalty level should also be reviewed.

Other Proposals on Strengthening the Protection of Data Subjects

The PCPD also made proposals which aim at enhancing the protection over data subjects. According to the existing Ordinance, a person who contravenes the data protection principles faces no sanction unless he does so in non-compliance with an enforcement notice issued by the Commissioner. Although an aggrieved individual may institute a civil claim against the data user under section 66 of the Ordinance to seek compensation, the Commissioner is not aware of any award of damages having been made by the court since the commencement of the Ordinance more than 12 years ago. It is obvious that there is no effective punishment or deterrent on those who knowingly or recklessly failed to comply with the requirements of data protection principles, thereby creating a risk that substantial damage or distress will be caused to other persons.

Therefore, the PCPD proposed to refer to the UK model, which confers power on the Commissioner to **impose a fine for serious contraventions of the data protection principles**, provided that the breaches are avoidable and give rise to enormous data protection risk. The approach targets on behaviours that reveal either a reckless disregard for the Ordinance's requirements or gross negligence in complying with the Ordinance's requirements. The PCPD also proposed to confer power on the Commissioner to **award compensation to the aggrieved data subjects**. A similar provision exists in the Australian Privacy Act. The PCPD also suggested that the Commissioner be empowered to **provide legal assistance** to persons who intend to institute legal proceedings according to section 66 of the Ordinance in due course.

PCPD Fully Supports Public Consultation

In order to introduce to all sectors the amendment proposals set out in the Consultation Document, the PCPD actively took part in all promotional functions, such as responding to questions raised by LegCo members on the Consultation Document at the LegCo House Committee meetings, explaining to District Council members the proposals and answering questions thereon, attending open forums held by the Constitutional and Mainland Affairs Bureau, and answering questions raised by the public. The PCPD also held seminars to introduce the amendment proposals set out in the Consultation Document.

In addition, the Commissioner was invited to meet people from all walks of life, and participated and attended seminars held by political parties, professional bodies and academic organizations to explain the amendment proposals and listen to opinions. Until now, the Commissioner and the PCPD staff have participated in more than seventeen public forums and seminars.

The consultation period closed on 30 November 2009. However, follow-up works including analyzing opinions from all sectors will continue. The PCPD also needs to provide the Government with support on relevant issues, and to opine on the drafting of the amended provisions until the amendment proposals are materialized.

The review of the Ordinance is of utmost importance. While the review of data protection laws is handled by local law reform commission in overseas countries, the PCPD, with limited resources available, takes the initiative to carry out a comprehensive review of the Ordinance. The effort to review and up-date the Ordinance gives public a better protection of personal data privacy to help them face the challenges of this electronic era.

Is It Worthwhile for the Commissioner to Initiate Ordinance Review?

A comprehensive review of the Ordinance is both significant and costly. In overseas countries, the work is often carried out by local law reform organizations and handled by experts and designated staff. Given the ten-year-plus history of the Ordinance in 2006, the considerable regulatory experiences accumulated, the problems encountered during its execution, and the personal data privacy issues to be encountered and addressed in tandem with technological advancement, the Commissioner considers it necessary to promptly and actively initiate a review on the Ordinance and submit proposals to government authorities.

The review of the Ordinance has lasted since 2006. The Commissioner counts on existing resources to handle the project greatly beneficial to the general public on top of his routine duties. With the efforts of its staff in carrying out studies and reviews, the PCPD managed to urge the Government to kick off a public consultation for the review of the Ordinance, quickening the pace of reform.

Chapter 8: Global Liaison and Cooperation

APEC ECSG Data Privacy Subgroup

Being the personal data privacy regulator in Hong Kong, the PCPD was invited by the Government to participate in the works of the Data Privacy Subgroup (“DPS”) of the Electronic Commerce Steering Group (“ECSG”) under the Asia Pacific Economic Co-operation (“APEC”) in 2003 to develop a **data privacy framework** recognized among member economies for the sake of promoting the development and launch of e-commerce, and building up consumers’ trust and confidence. Since then, the Legal Division of the PCPD has advised on the project and assisted the Commissioner in tackling personal data privacy issues.

The preliminary works of the DPS was to draft a set of **data privacy principles**. Hong Kong takes a leading role in Asia Pacific region in terms of personal data privacy protection. Hence, the PCPD offered professional opinions during the drafting of the information privacy principles in the capacity as a privacy regulator. The workload of the Subgroup was rather hefty. After endless discussions and amendments to the draft of the APEC Privacy Framework, the final version of the text was endorsed at APEC Ministers’ Meeting in 2004.

Thereafter, the Subgroup strived to work on issues in relation to the implementation of the privacy framework, including domestic as well as international implementation. As regards its implementation on the international front, the Ministers of APEC endorsed the Data Privacy Pathfinder in 2007 to join efforts in carrying out a number of projects aiming to develop an implementation mechanism built on the foundation of trust, with a view to ensuring the free flow of information across the Asia Pacific region. Projects under the **Data Privacy Pathfinder** include:

1. Self-assessment guidelines for business;
2. Trustmark (accountability agent) guidelines;
3. Compliance review process of Cross Border Privacy Rules;
4. Directories of compliant organizations;

5. Contact directories for data protection authorities and privacy contact officers within economies, as well as those of accountability agents;
6. Templates for enforcement cooperation arrangements;
7. Templates for cross-border complaint handling forms;
8. Guidelines and procedures for responsive regulation in Cross Border Privacy Rules system; and
9. A pilot program that can test and implement the results of the projects.

The Legal Division of the PCPD has participated in the telephone conferences of a number of project groups, and provided written comments on the draft of the document.

The year 2009 is of profound significance, which marks another milestone in DPS's works. The Subgroup strives to put into place the cross-border privacy cooperation arrangements, which the Subgroup has strived to put into place, was endorsed at the APEC Ministerial Meeting in November. All member economies are welcome to participate in the arrangements to promote cross-border cooperation on data privacy protection and handle complaints against any breach of data privacy.

In the meantime, the sheer popularity of the Internet means personal data can be disseminated abroad within seconds, and the flow of information is borderless. Therefore, it is necessary to study the adequacy of protection over citizens' personal data that are transferred abroad, which has to count on the cross-border cooperation among regions to develop data protection standard, and their concerted efforts in maintaining the standard.

The PCPD's participation in APEC's works allows it to more effectively reflect to the Government local data protection issues, and have a better grasp of the trends of data protection overseas, which helps bring into line the PCPD's enforcement of the Ordinance with the development of other regions. This not only benefits data subjects, but also helps data users (cross-border ones in particular) to handle personal data more properly in different jurisdictions with different legal systems.

Joint Efforts of Asia Pacific Privacy Authorities

The Commissioner also established partnerships with privacy authorities in the region to form the “Asia Pacific Privacy Authorities” aiming to exchanging opinions on privacy regulations, new technologies as well as the management of privacy enquiries and complaints. Member authorities meet twice a year. The PCPD hosted meetings in Hong Kong in November 2006 and June 2009 respectively. The aforementioned “Privacy Awareness Week” held annually since 2007 is another activity in the region which leverages joint efforts to promote personal data privacy.

Besides, the PCPD receives overseas personal data protectors, authorities and scholars from time to time to exchange work experience with them.

International Conference of Data Protection and Privacy Commissioners

This is the only global privacy forum. Privacy commissioners and data protection authorities over the world are invited to meet annually to discuss data protection issues of mutual concern. The Conference has two standing committees which the Commissioner is a member. In 2007, Hong Kong was honored to be appointed as one of the three members of the Credential Committee which is charged with the duty of handling applications for membership and making recommendations to the International Conference. In 2009, Hong Kong was re-elected a member of the same committee (the other two members are Spain and Ireland). Besides, Hong Kong has participated actively in consolidating the procedural and organizational arrangements for the future cooperation between members of the august body.

Forums Held by the Commissioner in Hong Kong

The Commissioner believes that where appropriate, he can act as a host for forums, inviting overseas privacy commissioners and experts to Hong Kong to attend so that the PCPD’s staff and the public can get familiar with the international privacy work, because an advice from others may help one’s defects.

In November 2006, the PCPD hosted the 26th Asia Pacific Privacy Authorities Forum and invited Privacy Commissioners of Australia and New Zealand to attend a public forum to discuss the issues of smart identity card and privacy safeguards of organizations.

In February 2008, the PCPD invited the privacy commissioners of the UK and British Columbia of Canada to attend a public forum to discuss privacy topics such as the installation of CCTV in public places and the handling of data leakage incidents.

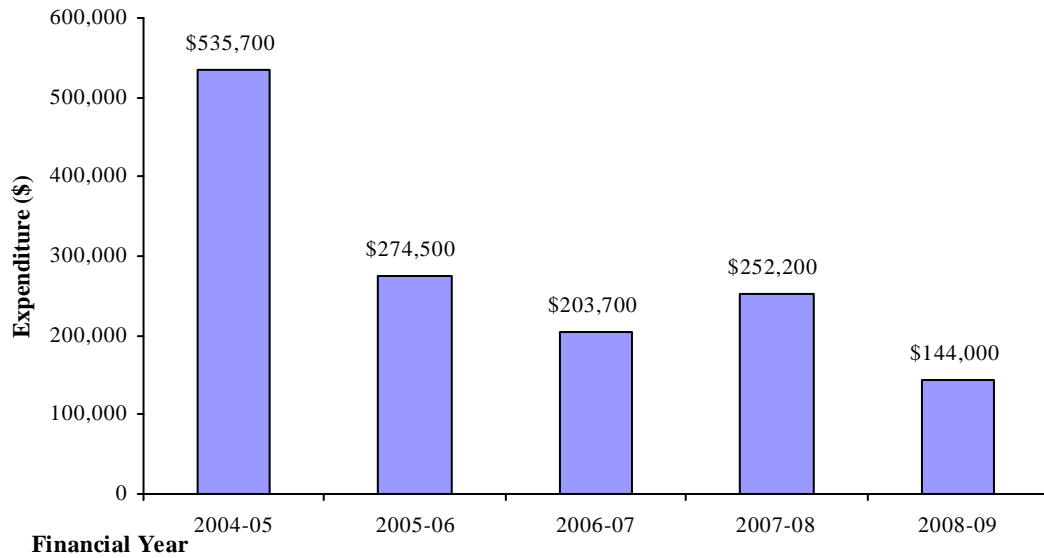
In June 2009, the PCPD invited the privacy commissioners of Australia, Canada and New Zealand as well as local experts to attend a public forum and hold a discussion on personal data privacy protection under the electronic health record sharing system. Representatives of privacy organizations in Macao and Portugal also attended the forum.

The Commissioner has tried his best to minimize the costs of these three forums. Though the PCPD has to bear part of the expenses of overseas speakers, the cost for each forum was between \$20,000 and \$50,000.

The Commissioner Minimizes Expenditure for Overseas Duty Visits

In the electronic era, the protection of personal data privacy is a global issue. As such, the PCPD has to maintain close ties with privacy jurisdictions in the globe and exchange experiences and insights with them to deal with local problems more effectively. To this end, the Commissioner considers it necessary to participate in relevant conferences and collaborations to perform his functions under the Ordinance. To cut back on expenses, the Commissioner has stuck to the principle of moderate and conservative when utilizing resources during overseas visits. As shown in **Fig. 12**, the expenses associated with overseas visits have been decreasing over the past five years, which clearly illustrates the PCPD's efforts in controlling expenses.

Fig. 12: PCPD’s Expenditure for Overseas Visits in the Past Five Years



PCPD’s Works Won Worldwide Reputation

The contributions made by the PCPD to promoting personal data privacy have won many accolades worldwide, which is best reflected in the letters issued to the PCPD by privacy regulators of different regions (see **Fig. 13**).

Fig. 13: Letters from overseas privacy regulators and the Chair of the APEC Data Privacy Sub-Group

“The task of a regulator can be a lonely affair. But it is greatly alleviated by establishing strong working relationships with other regulators. The Office of the Victorian Privacy Commissioner (Privacy Victoria) was established in July 2001. From its inception this office has greatly benefited from the wisdom and experience of the Hong Kong Privacy Commissioners of Personal Data and our offices respective staff have established excellent working relations. As we administer similar legislation and have similar functions we are able to share our thinking on many topics which has the added benefit of encouraging consistency of approach. In our early days we successfully adopted the Hong Kong initiative of having a Data Protection Officers’ Club and established our own Privacy Victoria Network of public sector privacy officers which continues to flourish. Since I was appointed Commissioner in March 2007 I have greatly benefited from being able to seek advice and exchange ideas with Mr. Woo, and other members of the Asia Pacific Privacy Authorities.”

Helen Versey
Privacy Commissioner
Office of the Victorian Privacy Commissioner, Australia

September 2008

23 September 2008

Dear Commissioner Woo

“I am writing to you as a dear and valued colleague.

Building on the previous good relationships between previous Hong Kong and Australian Commissioners since 1997, for over three years you and I have enjoyed an excellent productive working relationship. During this time we have worked collaboratively as members of the Asia Pacific Privacy Authorities Forum, in the implementation of the APEC Privacy framework and as part of the International Data Protection Commissioners Conferences. Our staff members have also forged links as we plan for Privacy Awareness Week and as we examine important global issues affecting the handling of personal information of our citizens. Our cooperative working relationship at the Commissioner and office level has been a highlight for me personally and I believe has seen witness to enhanced data protection outcomes.

I look forward to continuing our excellent collaboration.”

Karen Curtis
Australian Privacy Commissioner

“As Canada’s Asia Pacific province, British Columbia has strong social and economic ties with Hong Kong, and these are reflected in the long-standing connections between Hong Kong’s Office of the Privacy Commissioner for Personal Data and the Office of the Information and Privacy Commissioner for British Columbia. Hong Kong is fortunate to have an oversight agency that is active, innovative and highly respected internationally for its leadership in privacy enforcement. Our offices keep in close touch and we benefit a great deal from our relationship with our friends and colleagues in Hong Kong.”

David Loukidelis
Information and Privacy Commissioner for British Columbia, Canada
September 2008

“Through organizations such as the Asia-Pacific Economic Cooperation, Asia Pacific Privacy Authorities and the International Conference, you and your office play a very important role in helping to address international privacy issues.

In today's wired world, it is no longer possible to protect privacy on a country-by-country basis - international data flows are too great; technologies are evolving too rapidly; and jurisdictional challenges can seem too daunting. Given the growing importance of the Asia Pacific economies, your participation in the global privacy dialogue is critical.

I deeply value the relationship our two Offices have developed while working together to find global solutions for growing privacy challenges.”

Jennifer Stoddart
Privacy Commissioner of Canada
September 2008

“In a globalised world and an ever-expanding information society, the protection of personal data has become increasingly important. Data protection authorities around the world must therefore build alliances and work together in order to effectively protect personal data. I am therefore very pleased that the Hong Kong Privacy Commissioners' Office and the Dutch Data Protection Authority have solid and pleasant working relations. The Hong Kong Privacy Commissioner's Office is an important partner in Asia and I sincerely hope to be able to work closely together with my colleague in the years to come.”

Jacob Kohnstamm
Chairman, Dutch Data Protection Authority
September 2008

“In the age of globalization, cooperation between privacy commissioners from all continents has become most essential in protecting people's personal data privacy from the abuse of information technology and massive data flow.

The sharing of practices among commissioners has enhanced our ability and enabled us to deal with complaints about international data transfer more effectively. It also allows us to exchange views and reach consensus on topical privacy issues, which are constantly changing due to technological evolution, and have great impact on the ever-growing population in the world. We are very pleased that Hong Kong has joined the annual International Conference of Data Protection and Privacy Commissioners since the establishment of its office. At present, the Privacy Commissioners of France, Netherlands and Hong Kong form the Accreditation Committee in the International Conference and so we have a special working relationship.

As in every country with data protection law, the Privacy Commissioner in Hong Kong is obliged to maintain transparency by reporting its activities in the annual report, which is a fundamental guarantee of the independence that each Privacy Commissioner must demonstrate as a part of his duties. Sometimes it is hard to strike a balance between social and commercial interests. Every year we read Hong Kong's annual report with great

interest. We wish Mr Roderick WOO great success in his undertakings. He can count on our cooperation.”

Alex TÜRK, Chairman of the French Data Protection Authority,
Chairman of the European group of Data Protection Authorities established by the EU legislation,
General Secretary of the French Speaking “Association of Data Protection Authorities”

September 2008

“The need for personal information to be properly protected and for privacy to be adequately safeguarded has never been greater. Rapid developments with ever-cheaper technology, high-profile mistakes and scandals and the influence of dedicated Commissioners have transformed data protection into a truly mainstream issue. Everyone is now aware that concerns on the part of the public, the media and politicians have multiplied the reputational and regulatory risks of getting things wrong. On top of this, the march of globalisation has made data protection a truly international topic. The closeness of our respective approaches was really brought home to me during my visit in February 2008 alongside David Loukidelis, the Commissioner for British Columbia in Canada. The British and Hong Kong approaches especially have so much in common that it was such a rich and mutually educational visit for exchanging so much information about strategies and tactics for making the law work in practice.”

Richard Thomas
Information Commissioner
Office of the Information Commissioner, United Kingdom

September 2008

"Hong Kong's Personal Data (Privacy) Ordinance of 1996 which after the New Zealand's Privacy Act 1993 was the second privacy law outside Europe to cover the private as well as the public sector. Both laws are based on internationally accepted standards on fair information practices and are therefore very similar.

Over the years, the two privacy commissioners' offices have built a special relationship and have learnt much from each other. It has been useful for us to work together on many initiatives, for example on Asia Pacific Privacy Awareness Week, and in the contribution on Asia/Pacific approach to international privacy issues at the International Privacy Commissioners Conference. I firmly believe that this enduring relationship will enhance the protection of personal data across the region and beyond.
"

Marie Shroff
Privacy Commissioner, New Zealand
September 2008

" I am writing to you in my capacity as the Chair of the APEC Data Privacy Sub-Group. I have held the position of Sub-Group Chair since January 2007 and it is timely that I express my appreciation to you and your Office for your highly effective participation in the Sub-Group.

As you know, the Data Privacy Sub-Group was established in 2002 under the Electronic Commerce Steering Group. The role of the Sub-Group was to consider privacy issues in the context of the development of electronic commerce in the APEC region. APEC member economies recognised the enormous potential of electronic commerce to expand business opportunities, reduce costs, increase efficiency, improve the quality of life, and facilitate the greater participation of small business in global commerce. Economies also recognised the need for a framework to enable regional data transfers to benefit consumers, businesses and governments. To this end the Sub-Group developed the APEC Privacy Framework, which was endorsed by APEC Ministers and recognised by APEC Leaders in 2004.

The Sub-Group is currently working to implement the APEC Data Privacy Pathfinder, which was endorsed by APEC Ministers in 2007. The aim of the Data Privacy Pathfinder is to protect personal information which moves across borders in the APEC region by developing a system in which all APEC member economies may chose to participate. The Sub-Group has identified a number of Pathfinder projects addressing discrete elements of the proposed system. Hong Kong China has been a participant in the Data Privacy Pathfinder from the time of its endorsement by APEC Ministers in 2007.

In my view the active involvement of your Office in the work of the Sub-Group has made an important contribution to the success of the Sub-Group's work. As well as participating in the ongoing work of the Sub-Group, your Office's involvement has taken the form of participation in Data Privacy Pathfinder project groups which have met regularly by email and teleconference, as well as participation in the regular monthly teleconferences of Sub-Group members. Your Office has worked to develop and comment upon policy documents. This contribution has helped to ensure these policy documents recognise the different approaches of APEC member economies.

I have particularly valued your personal participation in the activities of the Sub-Group. My observation is that you have personally led the work of your Office and have brought to the Sub-Group your experience as a privacy regulator in the Asian region. In doing so, you have always clearly set out the parameters of your participation, noting that you are taking part as an independent regulator and not speaking on behalf of the Government of Hong Kong China.

Our work plan for 2010 is ambitious and will require the active and ongoing participation of all our experienced members. In conclusion, I hope that you will continue to be personally engaged with the work of the Sub-Group."

Colin Minihan
Chair
APEC Data Privacy Sub-Group
4 November 2009

Chapter 9: The Efficient Utilization of Resources by the Commissioner

When performing his functions, the Commissioner abides by the principle of proper and prudent use of public money. Since his assumption of office, the Commissioner noted a significant increase of privacy regulatory issues prompted by rapid changes in society which he has to handle within a tight budget at his disposal. Unlike other non government organizations which are not facing the same quandary, the Commissioner has to use extra efforts to find different ways to minimize expenditures in order to perform his functions effectively. The following are some examples:

1.	In early 2006, the tenancy agreement of the PCPD at Convention Plaza expired and the new monthly rent offered by the landlord was greatly increased to \$414,565. The Commissioner therefore decided to relocate the office to the present premises which attracted lower rental. When comparing with the rent offered for renewal of the tenancy, 7.5 odd million dollars were saved for the first three years of the lease.
2.	From 2003 to 2005, apart from following the salary reduction measures of the Government, the PCPD also froze the annual increment of its staff in order to save more resources.
3.	PCPD has gradually reduced the amount of gratuity upon renewal of employment contracts with staff who originally enjoyed a higher rate to the lower rate provided in the conditions of service of the newly recruited staff, and hence has cut the overall gratuity expenses of PCPD.
4.	The compensation of overtime work of some staff by monetary payments was abolished a year ago and instead time-off is given. As a result of the change, the Commissioner does not have the service of driver and motor car for some of the time.
5.	After assuming his office, the Commissioner exercised careful judgment about the representativeness and importance of different overseas privacy seminars and forums, and decided that there are three international conferences that must be attended. The number of overseas visits has greatly been reduced. The yearly expenditure dropped dramatically from the highest of \$578,960 (2001/02) to the lowest of \$144,000 (2008/09).

6.	After assuming his office, the Commissioner formulated internal guidelines requiring that flight mileage earned in duty travel shall be used to exchange for free air tickets for duty travel of the Commissioner and officers. Moreover, the Commissioner voluntarily travels on economy class for short flight. (Note: The rank of the Commissioner is entitled to business class in all flights.)
7.	After assuming his office, the Commissioner reviewed and amended the guidelines governing the provisions for duty passages. The accommodation of all officers going for overseas visits is standard room of a hotel, and no differential or better treatment is given to the Commissioner.
8.	Regarding minimizing the PCPD's hospitality expenses, the annual average expense before the Commissioner assumed office in 2005 was \$72,500, while the annual average expense after he assumed office was \$24,750. The highest amount of entertainment expense was \$127,915 (2001/02) and the lowest was \$16,788 in 2008/09. For the promotion and lobbying work to different stakeholders and influential persons in the community, the Commissioner has paid the expenses most of the time without seeking reimbursement from the PCPD.
9.	The Staff Welfare Fund of the PCPD was set up with the public money in 2002/03 and the average annual expense was \$37,200. After assuming his office, the Commissioner cancelled such fund and forbade the use of public money for holding farewell meals. He chose to pay most of the items himself that were previously paid out from the Staff Welfare Fund.
10.	In order to save expenses, the Commissioner cancelled the allowances for annual body check-up for himself and two staff members of directorate grade after assuming office.
11.	The Commissioner voluntarily subsidized staff who took flu vaccination.
12.	To save training expenses, the Commissioner invited local and overseas guests to provide training to PCPD's staff without charge. All the training was conducted in the PCPD's premises in order to save venue rental.
13.	To cancel the free parking provide to staff of directorate grade.
14.	To minimize the litigation costs paid to outsourced solicitors, the Commissioner has successfully persuaded some solicitors to substantially reduce their service fee.

15.	The Commissioner invited four experts to assist voluntarily in the inspection of Hospital Authority's Patients' Data System in 2008 and no consultancy fee was incurred.
16.	To minimize printing cost and postage, and to be environmentally friendly, the public is encouraged to browse PCPD's website for its publications. The number of hard copies printed for these publications will be reviewed periodically.
17.	<p>When launching industry-wide promotion activities, promotion expenses were shared with the partners, e.g.</p> <ul style="list-style-type: none"> ● Personal Data Privacy Campaign for Estate Agency Trade: the Estate Agents Authority agreed to pay half of the expenses, i.e. about \$50,000. ● "Care for patients – Protect their personal data" Campaign: the Hospital Authority agreed to pay half of the expenses, i.e. about \$100,000.
18.	Fully utilize free or inexpensive venues, e.g. PCPD's conference room, Multi Function Hall of Hong Kong Federation of Youth Groups, Hall of Duke of Windsor Social Service Building at Wanchai, Hall of Wah Yan College (the Commissioner's alma mater).
19.	To control the expenses incurred for holding international forums, e.g. in the 3 forums held in the past three years: (i) the 26 th Asia Pacific Privacy Authorities Forum in 2006; (ii) public forum attended by Richard Thomas, the then Information Commissioner of the UK, Mr. David Loukidelis, the Information and Privacy Commissioner for British Columbia (Canada) and the Commissioner in 2008; and (iii) the 31 st Asia Pacific Privacy Authorities Forum in 2009, the average attendance for each of these events was over 200 participants and the expenses were controlled within the range from \$20,000 odd to \$50,000 odd.
20.	To save cost, the Commissioner reviewed and selected another renowned independent accounting firm as PCPD's auditor which provides the same high quality service but at a significantly lower cost.
21.	To enhance staff morale, the Commissioner has set up the "Commissioner's Award : my most favorite workmate" at his own expense since 2006. The award winner is elected by votes of staff.

The Way Ahead

The Odds

The Privacy Commissioner for Personal Data is the only statutory Office charged with the protection of individuals' personal data in Hong Kong. The ultimate goal is to cultivate a society that respects and complies with the data protection principles, facilitating the free flow of data. This goal may be set back by the limited resources that were allocated by Government to meet the increased expectations of the public on the effective exercise of my regulatory functions and powers. The situation is aggravated by such uncontrollable factors such as the number and complexity of complaints received and the incidents of data security breaches that keep occurring. That is why my officers feel that they are working under constant pressure which can sometimes exceed what they can bear. That in some ways explained the personnel turn-over rate which in many cases could have been averted.

Against these odds, the strategies I have to employ are always forced upon me by circumstances, chiefly by the resources constraint and the expectation of the public which quite understandably do not take into account the former predicament.

My Strategies

The ideal world the Privacy Commissioner hopes to create is one where data users act with sufficient transparency and accountability, and where the data subjects are privacy aware and handle their personal data with intelligence and alertness.

I accept that there will always be a gap between realities and the idealistic, but the job of the Privacy Commissioner is to close that gap ceaselessly. Updating the law is essential and continuing public education is imperative. From day to day, people have to be reminded so that they don't sleep-walk into a society where the collection and use of personal data, if unchecked, can get out of control. Observed from the vantage of my Office which has accumulated the experience and expertise of some thirteen years and witnessing the advancement and popularisation of information technologies, I can see that Hong Kong, in common with other sophisticated cities and regions, is facing an unprecedented challenge in the form of a formidable invasion of personal data privacy.

To give due protection to the people of Hong Kong, the several essential functions of the Privacy Commissioner have to be reinforced in the following perspectives:

- (1) The promotion of privacy awareness among the public has to be broadened. The formula of targeting specific industries to promote compliance with the requirements of the Ordinance has proven to be effective and should continue at a faster speed if additional resources should become available;
- (2) Promotion and education should go hand in hand. To enhance people's privacy awareness, education on protection of personal data should be readily provided. Special attention should be given to young persons and it would be good if the schools can work together with the Privacy Commissioner in this. Senior citizens who were not born in the digital era will need assistance to guard against the abuse of their personal data. On the other hand, it is equally important to educate persons who are trusted with the handling of other people's personal data.
- (3) The Privacy Commissioner should be able to spend more time and efforts on playing the guidance role. Organizational data users should benefit more from a greater variety of guidelines and codes of practice. More interaction with large organizations is conducive to the building of a healthy privacy governance.
- (4) Prevention is always better than cure. The Privacy Commissioner should carry out more compliance checks to prevent recurrence of contraventions of data protection principles. More inspections of personal data systems should be carried out. This will result in constructive recommendations made to data users. In the handling of individual complaints, the policy should continue to be one of selectiveness. To some degrees, it is a judgment call on the part of the Privacy Commissioner to determine where the public interest lies in order to strike a proper balance on the efficient utilization of the limited resources.
- (5) In all enforcement actions, the principle of justice and fairness come into play. Where resources can be spared, it is a good plan to check on whether full compliance with the enforcement notices has been put into effect on an ongoing basis.
- (6) The Ordinance should be reviewed at timely intervals. This is desirable to see

that the requirements of the law have not been overtaken by fast developing information technologies and practices which may have adverse effects on the privacy of individuals in relation to personal data.

- (7) Hong Kong will do well to keep the high international and regional acclaim and to maintain the edge it has gained in both human rights and e-trade and commerce.

Significant Ongoing Projects

With such a small work force, it is imperative for the Privacy Commissioner to allow maximum flexibility in planning its work so that important projects can be undertaken on an urgent and priority basis. However, I can expect the future work programmes will include the following:-

- (1) To assist the Government to complete the legislative process in amending and updating the Ordinance. This should take the whole of 2010 and 2011.
- (2) To conduct first a Privacy Impact Assessment and then a Privacy Compliance Audit in respect of the Electronic Health Record Sharing Programme. This is likely to take more than five years from early 2010.
- (3) The implementation of the Data Users Registration Scheme. This may be accomplished within two years.

I predict that as time goes on many more new projects will emerge which require a positive input from the Privacy Commissioner. They are simply beyond what one can plot or plan.

The Right Ingredients to Success

I believe that the future success of the Privacy Commissioner will depend on some indispensable criteria including the following:-

The Independence of the Privacy Commissioner

The privacy law in Hong Kong, which is similar to those overseas where there are privacy commissioners, gives the Privacy Commissioner an independent status so that he does not operate within the governmental framework. This is as it should be because the various government departments and bureaux are data users and have to comply with the requirements of the Ordinance. The Privacy Commissioner can continue to exercise his investigative and enforcement functions fairly and equitably without fear or favour. The success and persuasive influence of the Privacy Commissioner will largely thrive on public confidence and trust.

Sufficiency of Operational Resources

With modern technological developments and widespread use of electronic and biometric devices in so many areas of human endeavours, a regulatory body simply cannot be expected to operate efficiently unless it has sufficient funding. After all, it has to tackle some state of the art data systems run by mega-size data users which may in some cases be a top bank or a leader in global tele-communication business. On the promotional and educational side, how I ever managed to get along with educating the masses with only just one full-time trainer is still a mystery to me.

It is simply not good enough to handle and protect the personal data of more than seven million people in this giant of a metropolis with only about 30 officers. The fundamental policy governing the allocation of funds to the Privacy Commissioner has got to be re-assessed. After all, it should be clear to most people that most human affairs nowadays involve personal data and personal data are omnipresent and proliferating.

A Permanent Office

It is in the public interest that the Government do seriously consider providing a fund to statutory bodies such as the Privacy Commissioner to acquire permanent office premises for they cannot be expected to move around like a gypsy forever gyrating to where the rent is the lowest. There is also the public to think of. They cannot be expected to keep track of the latest address of the statutory bodies they wish to visit for assistance.

Strengthening the Regulatory Regime

I expect the Ordinance review exercise carried out by the Constitutional and Mainland Affairs Bureau to speed up the pace of the legislative amendment process. The protection of the personal data of the individuals can then be brought up to date and strengthened while the Privacy Commissioner can work with a better set of tools.

Maintaining Hong Kong's Advantages and Competitiveness

With the globalization and the borderless flow of personal data, the Privacy Commissioner has to keep abreast of the international development in standard of privacy protection which is still in an evolutionary stage. Guidance should then be given to data users and data subjects alike to help them be more aware of the latest threats and risks in the areas of personal data privacy. It goes without saying that the Privacy Commissioner has to keep a close network with other data protection authorities and work in collaboration with them in areas of common interest.

Last, but most importantly, the Privacy Commissioner and its staff have to be committed to the work they do. Their hearts count as much as their heads in serving the public in this innovative area of human rights and facilitating the flow of data which is the backbone of 21st century businesses.

Roderick B Woo
Privacy Commissioner for Personal Data
December 2009

~ End ~