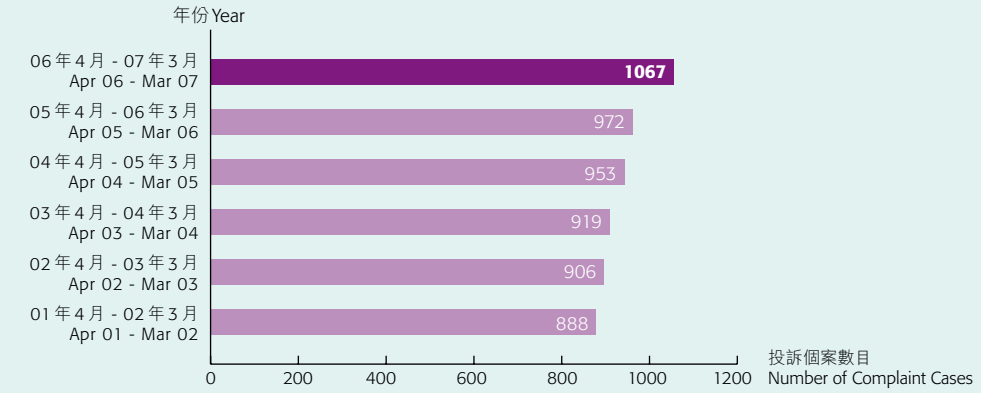
聆聽分析　保障市民利益

Listen and analyze　Protect privacy rights

調查投訴
Complaint Investigations

在二零零六至零七年度接獲的投訴個案
Complaints Received 2006-2007

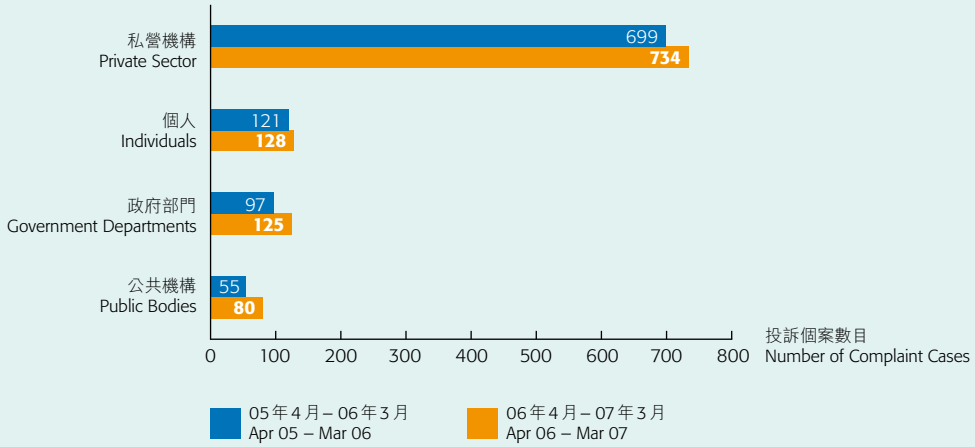
圖表1 — 每年的投訴個案
Figure 1 – Annual Complaint Caseload



在二零零六至零七年度公署共接獲1,067宗投訴個案(較去年上升了10%)。

A total of 1,067 complaint cases were received in 2006-2007 (an increase of 10% on the previous year).

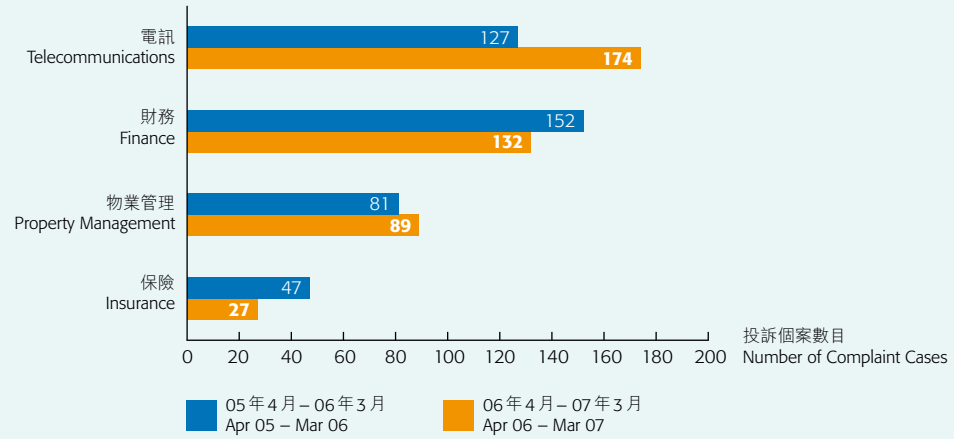
圖表2 — 被投訴者的類別
Figure 2 – Types of Party Complained Against



- 734宗(69%)個案投訴私營機構;
- 205宗(19%)個案投訴公營機構(即政府部門及其他公共機構);
- 128宗(12%)個案投訴個人。

- 734 (69%) complaint cases were against private sector organizations.
- 205 (19%) complaint cases were against public sector organizations (i.e. government departments and other public bodies).
- 128 (12%) complaint cases were against individuals.

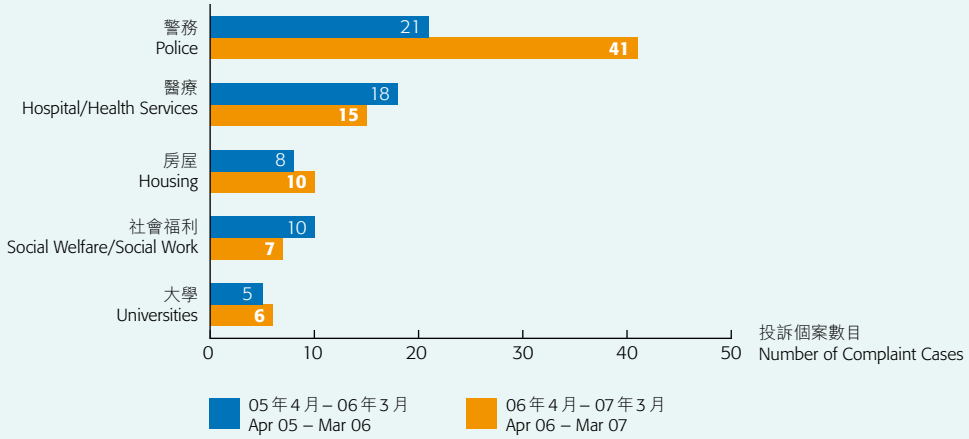
圖表 3 — 對私營機構的投訴
Figure 3 — Complaints Against Private Sector Organizations



在投訴電訊業及財務機構的個案中，大部分被指非法使用或披露客戶的個人資料。

The majority of complaints against the telecommunications and financial sectors alleged the unlawful use or disclosure of customers' personal data.

圖表 4 — 對公營機構的投訴
Figure 4 — Complaints Against Public Sector Organizations



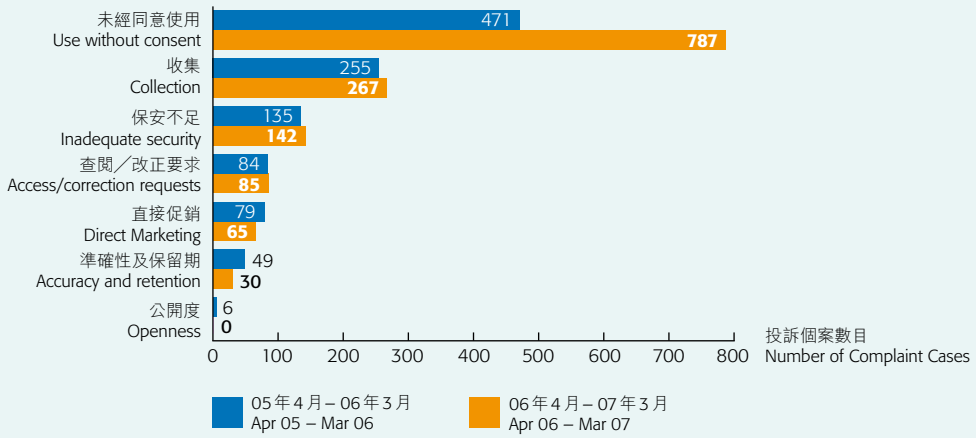
在投訴公營機構的個案中，大部分涉及：

- 被指與不符收集目的及未取得當事人同意而使用個人資料(51%)；
- 欠缺保障個人資料的保安措施(24%)；
- 未能遵守查閱資料要求或改正資料要求(13%)；及
- 過量或不公平收集個人資料(11%)。

The majority of complaints against public sector organizations involved:

- the alleged use of personal data beyond the scope of collection purpose and without the consent of the individual (51%);
- lack of security measures to protect personal data (24%);
- non-compliance with data access or correction requests (13%);
- and excessive or unfair collection of personal data (11%).

圖表 5 — 投訴的性質
Figure 5 — Nature of Complaints



二零零六至零七年度接獲的1,067宗投訴個案共涉及1,376項被指違反私隱條例的規定。在這些事項中，1,226項(89%)被指違反保障資料原則的規定，以及150項(11%)被指違反私隱條例的主體條文。

The 1067 complaint cases received in 2006-2007 involved a total of 1376 alleged breaches of the requirements of the Ordinance. Of these, 1226 (89%) were alleged breaches of the data protection principles and 150 (11%) were alleged contraventions of the provisions in the main body of the Ordinance.

在1,226項被指違反保障資料原則的事項中，787項(64%)涉及在未獲投訴人同意前，使用他們的個人資料。在這類個案中，75項(10%)涉及收債活動，大部分是財務機構及電訊公司被指將客戶的個人資料，例如聯絡資料及欠帳額，轉交追討欠款公司作追收欠債用途。

Of the 1226 alleged breaches of the data protection principles, 787 (64%) concerned the alleged use of personal data of complainants without their consent. In this category, 75 (10%) involved debt collection, mostly allegations against financial institutions and telecommunications companies for passing customers' personal data, such as contact details and amount of indebtedness, to debt collecting agencies for the recovery of outstanding debts.

有些投訴人對私隱條例在個人資料的使用及披露方面的適用範圍有所誤解。一個常見的例子是，有些投訴人認為只可在取得他們的特定同意後才可使用或向他人披露他們的個人資料。私隱條例限制個人資料只可使用或披露於原有收集目的或直接有關目的，其他的使用或披露必須經資料當事人的明示同意。換句話說，假如個人資料的使用或披露是在原有收集目的的範圍內，或為了直接有關的目的，則資料使用者便毋須在使用或披露前先取得資料當事人的同意。

There is a misunderstanding among some complainants regarding the ambit of the Ordinance when applied to use or disclosure of personal data. A common example is that some complainants believe their personal data can only be used or disclosed to others after prior consent concerning a particular act has been obtained from them. The Ordinance restricts the purpose of use or disclosure of personal data to their original collection purpose or a directly related purpose. Any other use or disclosure of personal data requires the express consent of the data subject concerned. In other words, if the use or disclosure of personal data is within an original collection purpose, or a directly related purpose, it is not necessary for the data user to obtain the consent of the data subject prior to use or disclosure.

調查投訴
Complaint Investigations

圖表6 — 二零零六至零七年度處理的投訴摘要
Figure 6 — Summary of Complaints Handled in 2006-2007

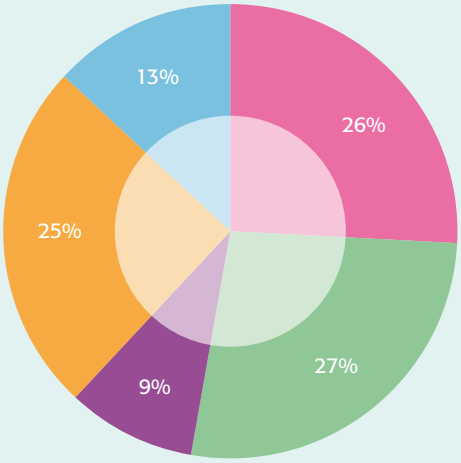
	2003-04	2004-05	2005-06	**2006-07**
上年轉來的投訴 Complaints carried forward	203	157	195	**188**
接獲的投訴 Complaints received	919	953	972	**1067**
經處理的投訴的總數 Total complaints processed	1122	1110	1167	**1255**
經審理後不再處理的投訴 Complaints screened-out	367	220	400	**542**
經審理後繼續處理的投訴 Complaints screened-in	755	890	767	**713**
完結 Completed	598	695	579	**525**
處理中 In process	157	195	188	**188**

在本年報期開始時，公署正處理上年度帶下來的188宗投訴，加上新收到的1,067宗投訴，私隱專員在本年報期內共須處理1,255宗投訴。在這些個案中，542宗(43%)經初步審閱後不獲受理，理由是其中的440宗的表面證據並不成立，無法支持有違私隱條例規定的指控，另外102宗不屬私隱專員的權力範圍。餘下713宗(57%)正在審閱中或經審閱後獲進一步處理，其中525宗(74%)在本年報期內已得到解決，而餘下的188宗(26%)在二零零七年三月三十一日時仍在處理中(圖表6)。

At the beginning of the reporting year, 188 complaints were being processed. With the 1,067 new complaints received, the Privacy Commissioner handled a total of 1,255 complaints during the reporting period. Of these, 542 (43%) cases were declined for further action after preliminary consideration because 440 of them were found to have no prima facie case to support allegations of breaches of the Ordinance, and the remaining 102 cases were outside the jurisdiction of the Privacy Commissioner. The remaining 713 (57%) cases were either in the preliminary screening process or screened-in for further consideration. Of these, 525 (74%) cases were resolved during the reporting year while the balance of 188 (26%) were still being processed on 31 March 2007 (Figure 6).

圖表 7 — 投訴結果
Figure 7 — Outcome of Investigations

證據不足 Unsubstantiated	26%
調解 Mediation	27%
撤回 Withdrawn	9%
其他規管機構處理 Other authority	25%
正式調查 Formal investigation	13%



在本年報期內完結的525宗個案：

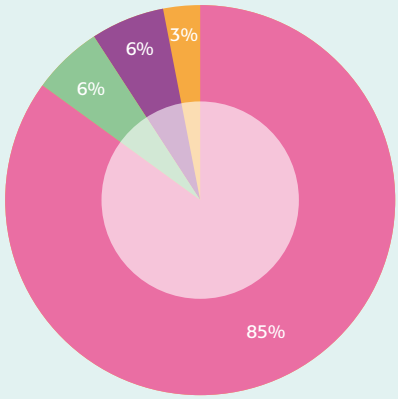
- 142宗(27%)透過調解得到解決；
- 70宗(13%)在進行正式調查後得到解決；
- 135宗(26%)在進行初步查詢後發現證據不足；
- 48宗(9%)在初步查詢期間由投訴人撤回；及
- 餘下的130宗(25%)投訴個案，大多涉及投訴人不回應私隱專員的查詢或個案已由其他規管機構，例如警方跟進。

Of the 525 cases completed during the reporting period:

- 142 (27%) cases were resolved through mediation;
- 70 (13%) cases were resolved after formal investigations;
- 135 (26%) cases were found to be unsubstantiated after preliminary enquiries;
- 48 (9%) cases were withdrawn by complainants during preliminary enquiries; and
- the remaining 130 (25%) cases involved mostly complaints where the complainants did not respond to the Privacy Commissioner's inquiries or where the matter had been transferred or reported to other authorities e.g. the Hong Kong Police Force.

圖表8 — 正式調查結果
Figure 8 — Results of Formal Investigations

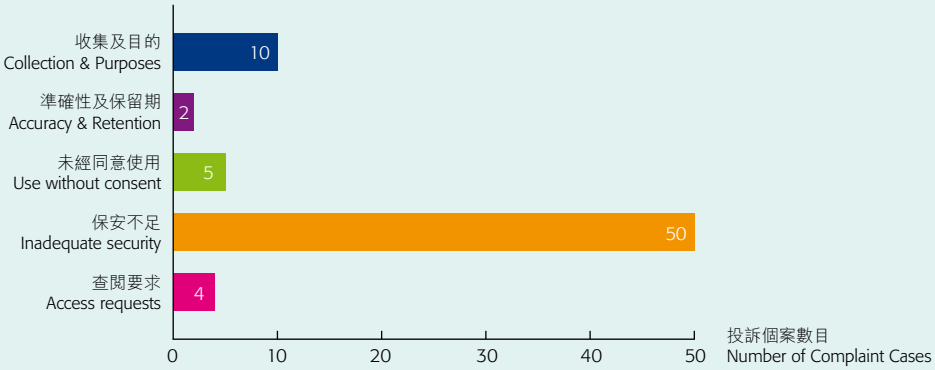
違反保障資料原則的規定 Contravention (Data Protection Principles)	85%
違反私隱條例主體條文的規定 Contravention (Provisions)	6%
無違例 No contravention	6%
中止調查 Discontinued	3%



在本年報期內完成正式調查的70宗個案中，私隱專員發現其中64宗(91%)違反了條例的規定，4宗(6%)並無違例或因缺乏證據而無法證明有違例情況。餘下2宗(3%)則是因投訴人決定不再跟進有關事項而中止調查。

Of the 70 formal investigations completed during the reporting period, the Privacy Commissioner found contravention of the requirements of the Ordinance in 64 (91%) cases. In four (6%) cases, either no contravention was found or contravention was not established due to insufficient evidence. The two remaining cases (3%) were discontinued as the complainant decided not to pursue the matter further.

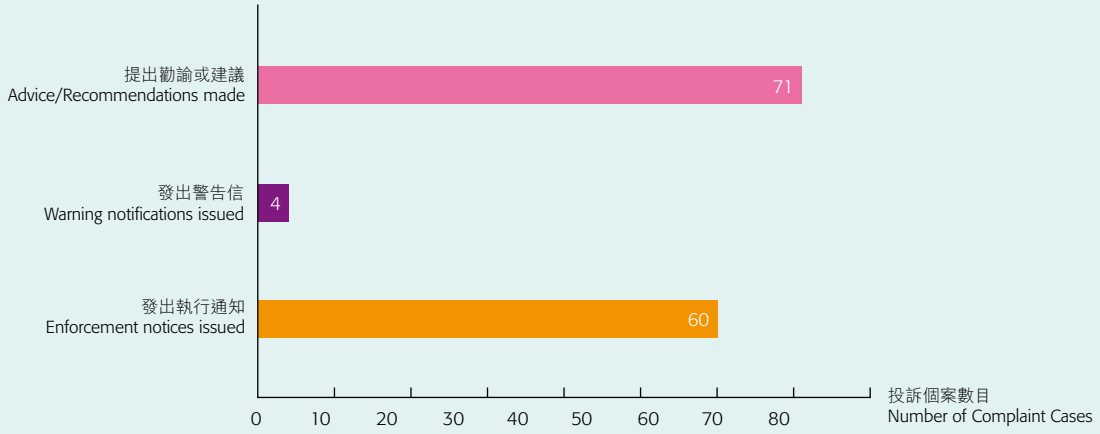
圖表9 — 違例事項的性質
Figure 9 — Nature of Contravention



在被確定違反條例規定的64宗個案中，60宗違反一項或以上保障資料原則，其餘4宗違反了條例主體條文的規定，當中所涉及的違例事項與依從查閱資料要求有關（圖表9）。

Of the 64 cases where the requirements of the Ordinance were found to have been contravened, 60 cases involved contravention of one or more of the data protection principles. The remaining four cases involved contravention of the requirements of the main body of the Ordinance relating to compliance with data access requests (Figure 9).

圖表 10 — 根據調查結果採取的行動
Figure 10 — Actions Taken as a Result of Investigation



在142宗透過調解得到解決的個案中，私隱專員向71間機構提出勸諭及／或建議，以協助它們在行事方式及程序上遵守保障資料原則及私隱條例的其他規定。

In the 142 cases resolved through mediation, the Privacy Commissioner provided advice and/or recommendations to 71 organizations on their practices and procedures in order to assist them in complying with the data protection principles and other requirements of the Ordinance.

在被確定違反條例規定的64宗個案中的60宗，私隱專員向被投訴的資料使用者發出執行通知，以防止它們繼續或重複違反規定。至於餘下的4宗個案，被投訴者已採取或書面承諾採取糾正措施，私隱專員因而毋須作出強制性行動，發出執行通知，而只是向有關資料使用者發出警告信。

Of the 64 cases in which requirements of the Ordinance were found to have been contravened, the Privacy Commissioner issued enforcement notices on the parties complained against in 60 cases to prevent continuation or repetition of the contraventions. In the remaining four cases, the parties complained against had either taken measures to remedy the contraventions, or given a written undertaking to implement them. As a result, enforcement action through the issuance of an enforcement notice was not necessary, and warning notices were issued.

重要的調查結果
Significant Investigation Results

下述投訴個案是本年報期內一些資料使用者被確定違反私隱條例規定的作為或行為。公署是基於有關事件的實況作出挑選，旨在述明受私隱條例（包括保障資料原則）管限的各種行為。

The following complaint cases illustrate some data user acts or practices that were found to have contravened the requirements of the Ordinance during the reporting period. They are selected on the basis of subject content and demonstrate the wide variety of conduct subject to the provisions of the Ordinance, including those of the Data Protection Principles ("DPP").

接受客戶以電話提出要求的公司：必須確保員工妥善核對來電者的身份及權力，以免帳戶持有人的資料外洩 — 保障資料第4原則

COMPANIES ACCEPTING REQUESTS FROM CUSTOMERS BY PHONE: MUST ENSURE PROPER VERIFICATION OF CALLERS' IDENTITIES AND AUTHORITIES TO AVOID LEAKAGE OF ACCOUNT HOLDERS' INFORMATION – DPP4

投訴內容

一間電訊公司的寬頻服務客戶不能以密碼進入其網上帳戶。她向該公司查詢後，發現曾有一名冒稱是她丈夫的男子致電客戶服務熱線，要求重新設定她的網上密碼。由於來電者能夠提供客戶的全名、香港身份證號碼及與客戶的關係，該公司於是按來電者的要求，把密碼重新設定為該客戶的香港身份證號碼首六個數字。

該公司解釋，上述做法是該公司對第三者代表帳戶持有人來電要求重新設定密碼時的標準核對程序。該公司堅稱，在程序中加入詢問帳戶持有人的地址已經可以保障帳戶持有人的個人資料私隱。

The Complaint

A customer using the broadband service of a telecommunications company could not log on to her internet account using her password. When she checked with the company, she discovered that a man pretending to be her husband had called the customer service hotline and requested that the account password be reset. Since the caller provided the customer's full name, Hong Kong identity card number and the relationship with the customer, the company agreed to his request and reset the password to the first 6 digits of the customer's Hong Kong identity card number.

The company explained that these measures were its standard verification procedure for handling such telephone requests. The company said that it would also ask for the account holder's address as an added safety measure.

結果

網上密碼是存取網上帳戶內個人資料的鑰匙，因此任何有關重新設定密碼的要求必須加倍小心處理，以免帳戶內的資料被未獲授權人士存取。

該公司詢問來電者帳戶持有人的姓名、香港身份證號碼、地址及與帳戶持有人的關係，並不足以確定該要求是否真的是由帳戶持有人作出或授權作出。把密碼重新設定為帳戶持有人的身份證號碼首六個數字亦不令人滿意。私隱專員認為該公司違反保障資料第4原則的資料保安規定，因為該公司的核對程序並不完善，沒有採取所有合理地切實可行的步驟，以保障客戶的個人資料免受未獲准許的存取。

私隱專員向該公司發出執行通知，指令它改善核對程序，確保重新設定網上帳戶密碼的電話要求確是由帳戶持有人作出或授權作出。該公司同意遵從執行通知的要求。

Outcome

An internet password gives online access to the personal data of an internet account. Any request to reset the password needs to be handled with extra care and caution to prevent access to the information by unauthorized people.

The company's practice of asking the caller for the account holder's name, Hong Kong identity card number, address and the caller's relationship with the account holder was plainly insufficient to determine whether the request is genuine and authorized. The resetting of the password to the first 6 digits of the account holder's identity card was also unsatisfactory. The Privacy Commissioner found that the company had contravened the security requirements of DPP4 in failing to take all reasonable practicable steps to protect customers' personal data against unauthorized access due to its inadequate verification procedure as aforesaid .

The Privacy Commissioner issued an enforcement notice against the company directing it to improve its verification procedure and ensure that any telephone request to reset internet account passwords was properly made or authorized by the account holder. The company agreed to comply with the enforcement notice.

提供網上賬單服務的公司：必須確保客戶的個人資料不被他人擅自取用 — 保障資料第4原則

COMPANIES PROVIDING ONLINE BILLING SERVICES: MUST ENSURE PERSONAL DATA OF CUSTOMERS ARE PROTECTED AGAINST ACCESS BY UNAUTHORIZED PERSONS – DPP4

投訴內容

有人發現在登入一間電訊公司的網上賬單系統後，即使用戶已登出系統、或瀏覽器被結束後重新啟動，仍然可以從瀏覽器的歷程記錄中檢索用戶的個人資料。

The Complaint

It was discovered that, after logging onto the online billing system of a telecommunications company, web pages containing customers' personal data could still be retrieved from the browser's history even after logging out of the system and/or restarting the browser.

結果

私隱專員調查發現，有關保安失誤是在用戶使用的電腦發生的，由於電腦的瀏覽器軟件的設定，使瀏覽過的網頁內的資料，被儲存於快取記憶體中。該電訊公司表示事後已採取措施堵塞保安漏洞。不過，只是建議客戶採用某一瀏覽器，而沒有通知他們不採用建議的瀏覽器可能涉及的風險是不足夠的。私隱專員認為該電訊公司沒有在客戶使用其網上賬單服務時採取所有合理地切實可行的步驟以保障客戶的個人資料，因而違反了保障資料第4原則的規定。

私隱專員向該電訊公司送達執行通知，要求它定期以市面上可獲得的新瀏覽器測試其網上賬單系統，並堵塞瀏覽器可能引致的資料保安漏洞。該電訊公司亦須要在客戶使用其網上賬單服務時通知他們若不使用建議的瀏覽器便可能涉及的風險。該電訊公司已遵從執行通知的要求。

Outcome

An investigation by the Privacy Commissioner revealed that the security lapse occurred at the user's accessing terminal where the user's browser software was configured to store personal information from the visited webpages in the cache memory. The telecommunications company stated that they had subsequently taken measures to stamp out the security loopholes. However, it was insufficient for the telecommunications company to simply recommend its customers to use a particular browser without advising them of the details of the risks that might entail for not using the recommended browser. The Privacy Commissioner found that the company had contravened the requirements of DDP4 by failing to take all reasonably practicable steps to protect the personal data of customers when using its online billing service.

An enforcement notice was served requiring the telecommunications company to carry out periodic tests of its online billing system by using new browsers and fixing any data security loopholes associated with the browsers. The telecommunications company was also required to notify its customers when using its online billing service of the details of the risks that might entail for not using the browser recommanded by it. The telecommunications company had complied with the enforcement notice.

收數公司東主：公開張貼諮詢人的個人資料屬違法 — 保障資料第3原則及第64(7)條

DEBT COLLECTION AGENT: PUBLIC DISPLAY OF REFEREE'S PERSONAL DATA IS ILLEGAL – DPP3 AND SECTION 64(7)

投訴內容

投訴人是一名欠款人的諮詢人，該欠款人曾向財務公司借貸，財務公司其後委託收數公司東主追討債款。該收數公司東主在追討債款的過程中，曾在投訴人的住宅大廈走廊張貼載有投訴人姓名的通告。

The Complaint

The complainant was a referee of a debtor who had borrowed money from a financial institution. In default of payment, the financial institution appointed a debt collection agent (the Agent) to recover the debt. The Agent posted various notices containing the complainant's name in the corridor of the building where he lived.

結果

經調查後，私隱專員查明該收數公司東主確有公開張貼有關通告，以及他並沒有就處理諮詢人的個人資料方面制定任何內部政策或程序。

私隱專員認為收數人只可使用諮詢人(即投訴人)的個人資料於聯絡或尋找欠款人的用途上，而非向諮詢人施壓還款；而以上述方式使用諮詢人的資料並不在其合理的預期之內。私隱專員認為該收數公司東主公開張貼投訴人的個人資料屬使用有關個人資料於當初收集目的以外的用途，因而違反了保障資料第3原則。

因此，私隱專員向該收數公司東主發出並送達執行通知，指令他停止公開張貼諮詢人個人資料的做法，並就處理諮詢人的個人資料制定政策及程序。

該收數公司東主沒有回應該執行通知，因而違反了條例第64(7)條，屬刑事罪行。該收數公司東主因此被檢控，其後在裁判法院定罪被罰款5,000港元。

Outcome

After investigation, the Privacy Commissioner found that the Agent did post up the notices, and did not have any internal policy or procedure regarding the handling of referee personal data.

The Privacy Commissioner took the view that a debt collector should only use the personal data of the referee (i.e. the complainant) in locating the whereabouts of the debtor rather than exerting pressure on the referee to repay the debt; and that it would not be within the reasonable expectation of the referee to have his personal data being used in such manner. The Privacy Commissioner found that the Agent had contravened DPP3 for using the complainant's personal data other than for the original collection purpose by displaying the complainant's personal data in public.

An enforcement notice was issued by the Privacy Commissioner directing the Agent to stop posting the referee's personal data in public and to develop policies and procedures for handling referees' personal data.

The Agent did not respond to the enforcement notice. As a result, he committed an offence by contravening the enforcement notice pursuant to section 64(7) of the Ordinance. The Agent was subsequently prosecuted in the Magistrates' Courts, convicted and fined $5,000.

持有個人資料的機構：不可為依從查閱資料要求而徵收超乎適度的費用 — 第28(3)條

ORGANIZATIONS HOLDING PERSONAL DATA: MUST NOT IMPOSE AN EXCESSIVE FEE FOR COMPLYING WITH DATA ACCESS REQUEST – SECTION 28(3)

投訴內容

一名家長代其子向以前就讀的學校提出查閱資料要求，所要求的資料載於查閱資料要求表格的附表。他投訴即使他把查閱資料要求的範圍縮小，該校仍然沒有依從他的要求。投訴人亦投訴，該校為依從他的查閱資料要求而徵收超乎適度的費用。

The Complaint

A parent on behalf of his son made a data access request (DAR) to his son's ex-school for personal data relating to his son as described in a list attached to his DAR form. He complained that the school had failed to comply with his DAR even after he had scaled down the scope of his DAR. The complainant also complained that the school had imposed an excessive fee for complying with his DAR.

結果

公署進行了調查。該校在回應查閱資料要求時，拒絕提供其中一項資料，理由是該項資料包含另一人的個人資料。不過，根據條例第20(2)條，該校應略去有關個人的姓名或辨別身份資料，以依從查閱資料要求。該校亦拒絕投訴人查閱一封由校長發出的信件，理由是投訴人之前已取得該信。鑑於投訴人並沒有在其查閱資料要求剔除此項早前已取得的個人資料，該校拒絕提供此項文件亦構成不依從查閱資料要求。根據以上所述，該校沒有依從查閱資料要求提供有關資料，違反了條例第19(1)條。

私隱專員在決定該校為依從查閱資料要求而徵收的費用是否超乎適度時，認為資料使用者只可以取回在依從查閱資料要求過程中涉及尋找、取出及複製所需資料的人工成本及實付費用。人工成本僅指處理尋找、取出及複製資料工作的文書或行政人員的正常薪金。徵詢法律意見涉及的金額、略去部分資料或篩選有關資料所花的時間，均不得收取費用。在這情況下，該校收取的費用由於是根據校長及其他高級職員的平均時薪計算，屬於超乎適度，違反條例第28(3)條。

公署向該校送達執行通知，要求它修改徵收的費用(不應超出尋找、取出及複製所要求的資料的人工成本及實付費用)，並向投訴人提供他要求查閱的個人資料。

Outcome

An investigation was undertaken by the PCPD. It transpired that in response to the DAR, the school refused to supply one of the requested items on the ground that it contained personal data relating to another party. However, according to s20(2) of the Ordinance, the school should comply with the DAR by omitting the names or identifying particulars of other individuals. Regarding an item in relation to a letter given by the headmaster, the school also denied the complainant's access to it on the ground that the complainant had already obtained the same before. In view that the complainant had not sought to exclude such personal data previously obtained in his DAR, the school's refusal to supply that requested document also constitutes non-compliance with the DAR. In view of the foregoing, the school have contravened section 19(1) of the Ordinance for not complying with the DAR in respect of these items.

In determining whether the fee imposed by the school for complying with the DAR was excessive, the Privacy Commissioner is of the opinion that the data user may be allowed to recover only the labour costs and actual out-of-pocket expenses involved complying with a data access request in so far as they relate to the location, retrieval and reproduction of the data requested. The labour costs should only refer to the normal salary of clerical or administrative staff who are able to handle the location, retrieval or reproduction work. No charge for the sum incurred for legal advice or the time spent in redacting data or deciding which personal data should be disclosed or refused to be disclosed. In the circumstances, the fee imposed by the school, which based upon an average hourly salary comprising those of the headmaster and other senior staff, was excessive contrary to section 28(3) of the Ordinance.

An enforcement notice was served requiring the school to revise the fee imposed so that it should not be more than the labour costs and out-of-pocket expenses incurred for the location, retrieval and reproduction of the requested data, and to supply the complainant with the personal data requested in his DAR.

進行推廣活動的公司：必須確保員工切實核對「拒絕再接收促銷訊息」名單 — 第34條

COMPANIES CARRYING OUT MARKETING ACTIVITIES: MUST ENSURE PROPER CHECKING OF OPT-OUT LIST – SECTION 34

投訴內容

一名獨資經營者投訴一間電訊公司，儘管他已經提出口頭及書面的「拒絕再接收促銷訊息」要求（下稱「拒絕要求」），該公司仍然多次致電其公司的固網電話，進行直接促銷。

The Complaint

A sole proprietor complained that a telecommunications company was repeatedly making direct marketing calls to his office fixed line telephone, even though he had made both verbal and written opt-out requests.

結果

該電訊公司解釋，他們在互聯網上的一個商業電話指南中取得一間公司的名稱，以及公司代表（即投訴人）的姓名和電話號碼。雖然他們已經在收到投訴人的拒絕要求後把他的姓名列入「不要致電」的名單中，但電話促銷員（該電訊公司分判商的僱員）沒有核對有關名單，繼續向投訴人發出促銷電話。不過，該電訊公司辯稱在直接促銷電話中使用的資料是關於投訴人的獨資經營公司，而不是投訴人本身，故此該等資料並不屬於條例所訂明的「個人資料」。

私隱專員認為，根據條例第34(2)條，如果促銷電話是以某一特定人士為對象的話，便屬於「直接促銷」的定義。條例並沒有為「人士」一詞下定義，但根據《釋義及通則條例》第3條，它的意思包括「法團或並非

Outcome

The telecommunications company explained that they had obtained the company name and the name and telephone number of the company's representative, i.e. the complainant, from a business telephone directory on the internet. Although they had put the complainant on a "not-to-call" list upon receipt of his opt-out request, the telemarketers, who were the employees of a sub-contractor of the telecommunications company, failed to check the "not-to-call" list and continued to make marketing calls to the complainant. The telecommunications company argued that the data used in the direct marketing calls, which relates to the sole proprietorship, rather than the complainant, were not "personal data" as prescribed by the Ordinance.

The Privacy Commissioner was of the view that according to section 34(2) of the Ordinance, if the marketing call was made to a specific person it would fall within the definition of "direct marketing". The term "person" is not defined in the Ordinance but according to the definition under section 3 of the Interpretation and General Clauses Ordinance, it

法團組織的任何…團體」。獨資經營的業務屬於非法團組織的團體。因此，該電訊公司宣稱向投訴人的獨資經營公司作出的促銷電話，是可構成條例第34條下的「直接促銷」。另外，有關資料包括投訴人的姓名和電話號碼，是與投訴人有關的，因此屬他的個人資料。

means and includes "… any body of persons, corporate or unincorporated…". A sole-proprietorship is caught by the category of a body of persons unincorporated. The marketing calls made by the telecommunications company purportedly to the complainant being a sole proprietor amounted to "direct marketing" under section 34 of the Ordinance. Moreover, the data comprising the complainants' name and telephone number did relate to the complainant, hence constitute his personal data.

公署向該電訊公司發出書面警告，要求他們停止向投訴人發出直接促銷電話。

The PCPD issued a written warning to the telecommunications company requiring them to cease making direct marketing calls to the complainant.

在公署發出書面警告之後數星期，該電訊公司在一個月內最少曾向投訴人發出四次促銷電話。公署於是把個案轉交警方提出檢控。該電訊公司被票控四項違反條例第34條的罪名。在求情時，該電訊公司表示有關電話是由深圳分判商的僱員發出的，他們在致電之前並沒有核對「拒絕再接收促銷訊息」名單。就該四項傳票，裁判官裁定該電訊公司有罪，共罰款14,000元。裁判官亦表示，此等促銷電話「令人討厭及煩擾」。

A few weeks after issuing the written warning, the telecommunications company made at least four marketing calls within a month to the complainant. The PCPD referred the case to the police for prosecution. Four summonses were issued against the telecommunications company for contravening section 34 of the Ordinance. In mitigation, they stated that the marketing calls were made by employees of their sub-contractor in Shenzhen, who failed to check the opt-out list before making the calls.

The magistrate convicted the telecommunications company of the four summonses and imposed a total fine of $14,000. He also remarked that the marketing calls were "disgusting and annoying".

根據《個人資料(私隱)條例》第48(2)條發表的報告

《個人資料(私隱)條例》(下稱「條例」)第48(2)條訂明，私隱專員在完成一項調查後，如認為如此行事是符合公眾利益的，可發表報告(下稱「報告」)，列明該項調查的結果及由該項調查引致的、私隱專員認為適合作出的任何建議或其他評論。

在本年報期內，私隱專員發表了兩份報告，分別是關於：

(i) 資料使用者聘用外判資訊科技承辦商時必須採取保安措施以保障個人資料；及

(ii) 電郵服務提供者向中國執法機構披露電郵用戶的個人資料。

REPORT PUBLISHED UNDER SECTION 48(2) OF THE PERSONAL DATA (PRIVACY) ORDINANCE

Section 48(2) of the Ordinance provides that the Privacy Commissioner may, after completing an investigation and if he believes that it is in the public interest to do so, publish a report ("Report") disclosing the investigation results and any recommendations or comments that he sees fit.

During the reporting year, the Privacy Commissioner published two Reports respectively relating to:

(i) the security measures that have to be taken by data users to protect personal data when outsourcing IT work; and

(ii) the disclosure of an email subscriber's personal data by service providers to PRC law enforcement agencies.

聘用外判資訊科技承辦商時必須採取保安措施以保障個人資料

2006年10月26日，私隱專員就「投訴警方的公眾人士的個人資料在互聯網外洩」一事發表調查報告。

背景

事件最初在2006年3月10日由一份本地報章披露。投訴警方獨立監察委員會（下稱「警監會」）所持有約二萬名曾投訴警方的公眾人士的個人資料被放於互聯網上，公眾得以查閱。私隱專員隨即於2006年3月15日主動展開正式調查。調查展開之後，私隱專員共接獲55宗對警監會的投訴。調查方法包括到訪警監會辦事處、到訪投訴警察課、會見有關人士、向有關各方錄取口供、審查有關各方的文件記錄和書面陳述，以及口頭訊問根據條例第44條傳召的人士。

報告詳述管理投訴警察個案的系統、警監會的資訊科技系統、保安及私隱政策、引致互聯網上資料外洩的連串事件，以及私隱專員的調查結果和建議。

私隱專員的調查結果

私隱專員認為警監會違反條例附表1的保障資料第4原則的規定。保障資料第4原則訂明，資料使用者須採取所有合理地切實可行的步驟，確保其持有的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除或其他使用所影響。這原則要求資料使用者對其持有的個人資料採取保障及預防措施。保安級別應反映資料的敏感程度及違反保安規定可引致的損害程度。

Security Measures to Protect Personal Data when Outsourcing IT work

On 26 October 2006, the Privacy Commissioner published a Report of the findings of an investigation into the disclosure of personal data on the Internet of complaints made against the Police by the public.

Background

The incident was first reported in a local newspaper on 10 March 2006. The personal data of about 20,000 people, who had made complaints against the Police, held by the Independent Police Complaints Council ("IPCC") were posted on the Internet and were publicly accessible. The Privacy Commissioner carried out an investigation on 15 March 2006. Subsequently, the Privacy Commissioner received 55 complaints against the IPCC. The investigation was conducted through visits to the IPCC office, the Complaints Against Police Office, interviews with the people concerned and the collection and examination of statements, documents, records, written representations as well as oral examination of persons summoned under section 44 of the Ordinance.

The Report provided an account of the system of managing complaints against the Police; the IPCC's information technology system, security and privacy policies; events leading to the leakage on the Internet; and the Privacy Commissioner's findings and recommendations.

The Privacy Commissioner's Findings

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

私隱專員的調查結果發現警監會沒有採取：

(i) 任何步驟，以防止在沒有考慮是否屬必要的情況下而發放有關資料予外判資訊科技承辦商；

(ii) 任何預防措施，保障發放予外判承辦商的資料；以及

(iii) 任何切實可行的步驟，確保能查閱資料的人的良好操守、審慎態度及辦事能力，

導致資料在互聯網上外洩。

The basis of the findings was that the IPCC had failed to take: –

(i) any steps to prevent the data from being released to the IT contractor without due consideration of the necessity to do so;

(ii) any precautionary measures to safeguard the data that had been released to the contractor; and

(iii) any practicable steps to ensure the integrity, prudence and competence of persons having access to the data,

resulting in the leakage on the Internet.

執行通知

私隱專員根據條例第50條行使權力，於2006年9月18日向警監會發出執行通知，指示警監會於2006年10月16日前作出下列事宜：

1. 制定所需政策及實務指引，列明與外判承辦商或代理交往時，須妥善處理及保障投訴資料；

2. 實施有效措施，確保員工遵從這些政策及指引；以及

3. 檢討現時的外判合約，盡量在合約中加入條款，訂明承辦商須採取的措施，保障警監會交給他們的投訴資料。

私隱專員欣悉警監會已於2006年10月16日完全遵從執行通知的規定。

Enforcement Notice

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

1. Devise the necessary policy and practical guidelines for the proper handling and protection of the data when dealing with an outsourced contractor or agent;

2. Implement effective measures to ensure compliance by its staff with those policy and guidelines; and

3. Review the existing outsourcing contracts and endeavor to include in the terms measures to be taken by the contractors to protect the complaint data passed to them by the IPCC.

The Privacy Commissioner was pleased to note that on 16 October 2006, the IPCC had complied fully with the enforcement notice.

事件的教訓

從這件不幸事件汲取的教訓是，資料使用者處理敏感或大量的個人資料時，特別是電子形式，應該提高警覺。如他們要向外判承辦商或代理發放載有個人資料的資料庫時，應該採取預防措施，防止資料外洩。

Learning from this incident

This incident is unfortunate but offers many lessons. Data users should be alert about handling sensitive or large amounts of personal data, particularly if in electronic media. If they are asked to release personal data to an outsourced contractor or agent, precautionary measures should be taken to prevent any data leakage.

電郵服務提供者向中國執法機構披露電郵用戶的個人資料

2007年3月14日，私隱專員就「香港一個電郵服務供應商被指稱披露其用戶的個人資料」一事發表調查報告。

調查發現該供應商並無違反條例，不過此事件引致對條例的適用範圍的關注。

背景

2005年10月，本地報章報導一名內地記者X先生被中國法院裁定犯了為境外提供國家秘密罪。一個香港電郵服務供應商—雅虎香港有限公司（下稱「雅虎香港公司」）被指稱曾向中國執法機關披露X先生的個人資料，導致X先生被捕及被判刑。

由於電郵服務供應商收集及持有大量電郵用戶的個人資料，此事件引起公眾關注電郵用戶個人資料的保安問題，尤其是有關披露是為了遵從外地機關為調查該地罪行而根據該地法律發出的合法命令。

私隱專員的行動

2005年10月21日，私隱專員主動查看事件是否有涉及違反條例的情況。其後，私隱專員收到X先生的獲授權代表的投訴，指稱雅虎香港公司未經X先生同意，便向中國機關披露X先生的個人資料。私隱專員於2006年5月9日決定依據條例第38條進行調查。

調查

調查重點是要找出雅虎香港公司曾否披露X先生的個人資料；如有的話，有關披露是否違反了條例的保障資料第3原則；以及有關披露能否根據條例第58條獲得豁免。

The Disclosure of an Email Subscriber's Personal Data by the Service Provider to PRC Law Enforcement Agency

On 14 March 2007, the Privacy Commissioner published a Report detailing the results of an investigation into the alleged disclosure by an email service provider in Hong Kong of an accountholder's personal data.

The investigation found no contravention of the Ordinance but raised some concern about the scope of application of the Ordinance.

Background

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

As email service providers collect and maintain a large amount of email accountholder personal data, this incident highlighted the public's concern about the protection of subscribers' personal data privacy. In particular, there was concern about disclosing data to comply with a lawful order issued by a foreign authority to investigate a foreign crime.

The Privacy Commissioner's action

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

The investigation

The focus of the investigation was on whether any personal data of Mr. X was disclosed by YHKL; if yes, whether the disclosure had contravened DPP3 of the Ordinance; and whether such disclosure could be exempted under section 58 of the Ordinance.

調查過程困難是因為缺乏投訴人提供的證據，而所收集到的資料或證據亦有限。由於雅虎中國（由雅虎香港公司擁有）就業務運作而收集、持有、處理及使用有關個人資料的作為明顯是在中國發生，私隱專員曾就中國法律的適用問題向兩位中國法律專家徵詢意見，亦就條例的適用範圍向一位本地資深大律師徵詢意見。

The investigation proved difficult due to the lack of supporting evidence provided by the complainant, and the limited information available. As the act of collecting, holding, processing and use of the personal data by Yahoo! China, which is owned by YHKL, apparently took place in the PRC, legal advice was sought from two PRC law experts on the applicability of the PRC laws and from a local Senior Counsel on the scope of application of the Ordinance.

調查結果

私隱專員在考慮個案的所有情況後，最後認為沒有足夠證據證明雅虎香港公司披露了X先生的個人資料予中國機關。因此，雅虎香港公司並沒有違反條例的規定。

（私隱專員曾考慮的法律理據涉及事實與法律等錯綜複雜的問題，有關詳情，請參閱報告內容。）

調查的結果是無須發出執行通知。

Findings of the investigation

Having considered all the circumstances of the case, the Privacy Commissioner concluded that there was insufficient evidence to prove that Mr. X's personal data was disclosed by YHKL to the PRC authorities. Hence there had been no contravention of the requirements of the Ordinance by YHKL.

(For details of the legal grounds considered by the Privacy Commissioner, which involved questions of facts and laws, please refer to the body of the Report.)

No enforcement notice was issued as a result of the investigation.

調查引申的評論

本調查個案突顯對下述問題尋求明確答案的需要：

(a) 如個人資料的收集、持有、處理及使用作為全不是在香港進行，條例是否適用？

(b) 如個人資料的披露是為了遵從外地機關為調查該地罪行而根據該地法律發出的合法命令，條例的豁免條款是否適用？

就條例的詮釋及適用範圍作更清晰的界定，能有效提高個人資料私隱的保障。為此，公署正建議對條例進行檢討，希望政府配合法例修訂的過程。

報告可以在公署的辦事處（香港灣仔皇后大道東248號12樓）索取，亦可以從公署的網站（www.pcpd.org.hk/chinese/publications/invest_report.html）下載。

Privacy Commissioner's comments arising from the investigation

The investigation of the case highlights the need to clarify the following:

(a) Should the Ordinance apply where none of act of collection, holding, processing and use of the personal data takes place in Hong Kong?

(b) Should the exemption provisions in the Ordinance apply when the disclosure of personal data is made to comply with a lawful order issued by a foreign authority under foreign law to investigate a foreign crime?

A clearer interpretation and application of the Ordinance would enhance its overall effectiveness in the protection of personal data privacy. To this end, the PCPD is proposing a legislative review of the Ordinance and hopes the Government will facilitate the legislation amendment process.

Copies of the Reports are available from the PCPD at 12/F., 248 Queen's Road East, Wan Chai, Hong Kong. They are also available for download from the website of the PCPD (http://www.pcpd.org.hk/english/publications/invest_report.html).