PCPD NEWS
私隱專員公署通訊
二零一四年十二月 December 2014 | ISSUE NO. 30

專題報道
流動應用程式私隱風險

Cover Story
Privacy Risk of Mobile Applications

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

流動應用程式私隱風險
Privacy Risk of Mobile Applications

公署今年抽查60款由本地機構開發的熱門流動應用程式(「程式」),結果顯示這些程式的私隱政策透明度表現明顯不足,而與2013年同樣的抽查比較亦無顯著改善。

今次抽查是響應「全球私隱執法機關網絡」(Global Privacy Enforcement Network)於今年五月舉行的全球聯合行動。公署聯同25個私隱執法機關抽查程式的私隱政策透明度及讀取資料的權限。

今次全球性的抽查行動於2014年5月12日至18日期間進行,參與的私隱執法機關共抽查了1,211款流動應用程式,當中包括Apple及Android的程式、免費及付費的程式,以及公、私營機構的程式,而且種類廣泛,包括遊戲、健康/健體、新聞、銀行等。抽查重點是查看程式所要求的讀取資料權限種類,及這些權限相對這些程式功能是否超乎適度;而最重要的是,這些程式如何向用戶解釋為何需要讀取權限上提及的個人資料,及準備如何使用有關資料。

公署於12月15日舉行記者會,公佈本地流動應用程式私隱政策透明度的抽查結果。私隱專員表示:「要尊重用戶的私隱,透明而公開的政策是必須的。機構建立具透明度的私隱政策,讓用戶明白其個人資料在網上是如何被處理,至為重要。無可否認,要向程式用戶提供私隱資訊殊不容易,因為流動裝置的螢幕細小,用戶多數不會專注閱讀,但開發商遵從條例,責無旁貸。」

不過,國際抽查行動亦發現一些良好行事方式的例子:

- 15%的程式有清楚解釋他們會如何收集、使用及披露個人資料。私隱保障做得最好的程式在尋求每一項權限時,都會簡潔、易明地解釋會否收集及使用用戶的有關個人資料。
- 程式使用彈出資訊、分層資訊和及時通知,讓用戶能適時知道他們的個人資料將被收集或使用。

值得留意的是,在電子市場中非常受歡迎的程式,有部份亦是在私隱透明度方面最獲好評的。由此可見,程式如能向用戶講解清楚,即使會收集資料,亦不會對下載量有負面影響。

2014年智能手機應用程式抽查報告:私隱政策透明度 www.pcpd.org.hk/tc_chi/resources_centre/publications/surveys/files/sweep2014_c.pdf

The PCPD conducted a survey of 60 popular mobile applications ("apps") developed by Hong Kong entities and found that their transparency in terms of privacy policy was clearly inadequate and there was no noticeable improvement compared with the results of a similar survey conducted in 2013.

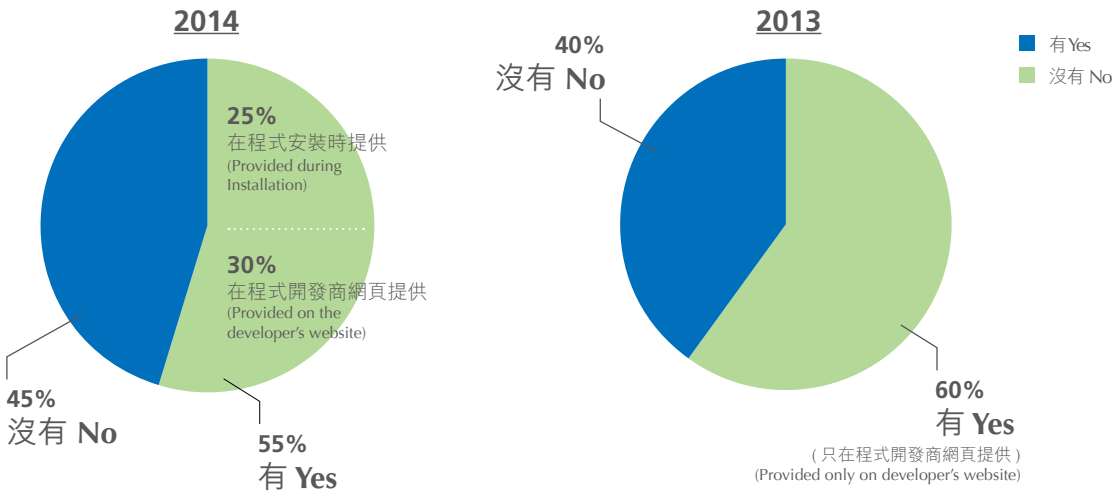
This year's survey was part of the Global Privacy Enforcement Network ("GPEN") mobile Sweep ("Sweep") exercise that took place in May this year. PCPD joined forces with 25 other privacy enforcement authorities around the globe to look at the privacy transparency and permission of apps.

The Sweep was conducted from 12 to 18 May 2014. In total, 1,211 apps were examined by all participating authorities included a mix of Apple and Android apps, free and paid apps, and public and private sector apps that ranged from games and health/fitness apps, to news and banking apps. The sweepers looked at the types of data access permissions the apps were seeking, whether the permissions exceeded expectations based on

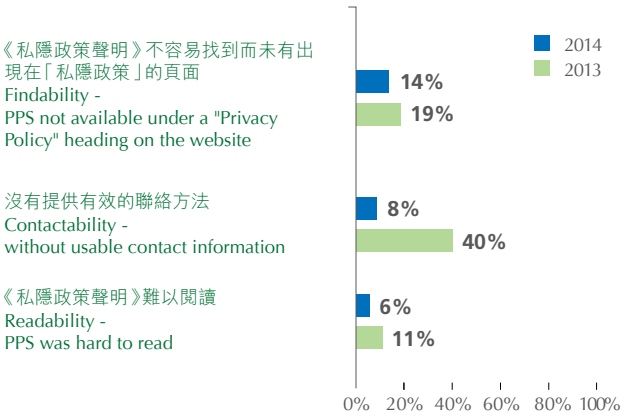
---

本地手機程式私隱透明度的調查結果如下:—
Major findings were: -

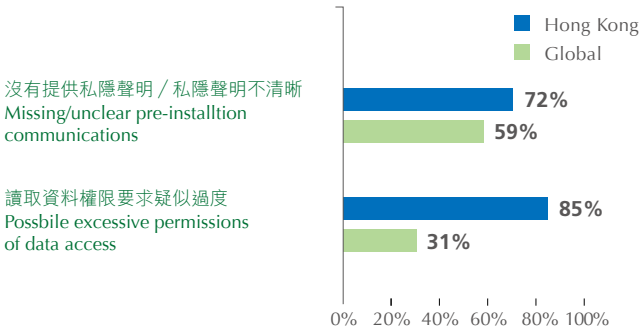
有沒有提供私隱政策聲明?
No. of apps provide PPS



私隱政策聲明的清晰度
Level of Transparency



讀取資料權限的清晰度及範圍
Transparency and Scope of Data Access Permission



the apps' functionality, and most importantly, how the apps explained to consumers why they wanted the personal information and what they planned to do with it.

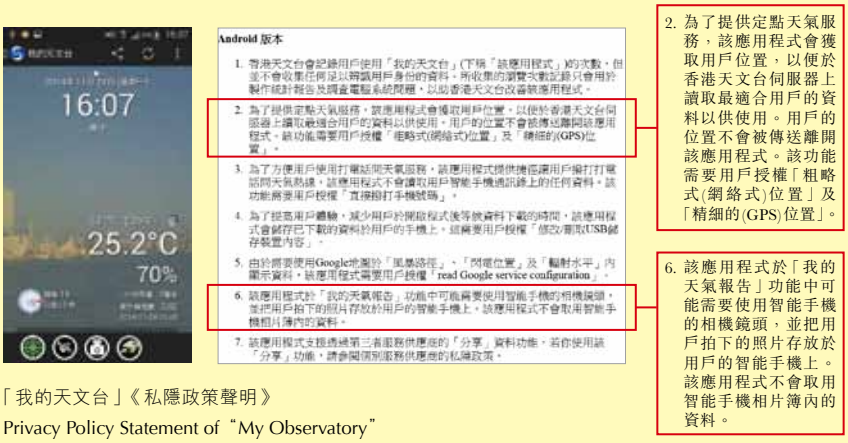
A press conference was held on 15 December to announce the results of the Sweep with respect to local mobile apps. The Commissioner commented, "Transparency is central to respecting the privacy of individuals and it is paramount that organisations develop transparent online privacy policies so that individuals understand how their personal data is handled in this virtual context. Admittedly, conveying privacy information to consumers can present unique challenges in the app world, where screens are small and users' attention can be intermittent. That said, compliance with the legal obligations under the Ordinance is a must."

On the other hand, some examples of best practices are noted in the international Sweep:

- 15% of apps provided a clear explanation of how they would collect, use and disclose personal information. The most privacy friendly apps offered brief, easy-to-understand explanations of what the app would and would not collect and use pursuant to each permission.
- Pop-ups, layered information and just-in-time notification were used to inform users of potential collections or uses of information when they were about to happen.

It is important to note that some highly popular apps in the e-marketplace were among those that received top ratings in transparency, demonstrating that when properly explained to consumers, the collection of information does not negatively impact on downloads.

2014 Study Report on the Privacy Policy Transparency of Smartphone Applications
www.pcpd.org.hk/english/resources_centre/publications/surveys/files/sweep2014_e.pdf



「我的天文台」《私隱政策聲明》
Privacy Policy Statement of "My Observatory"

公署認為「我的天文台」程式是值得參考的。該程式提供了易於理解的《私隱政策聲明》，顧及用戶的需要，說明會讀取及不會讀取的資料。而且，儘管Android 版本在安裝程式時已取得位置資料的權限，但其後仍讓用戶選擇容許或不容許該程式讀取位置資料。這例子正好證明開發受歡迎、實用及保障私隱的程式是可行的。

PCPD was impressed by the app MyObservatory as it featured an easily understandable PPS that addressed the concerns of users by articulating what data it would and would not access. Furthermore, the Android version facilitated users to allow or disallow location information to be read by the app, even though such permission had already been obtained at the time of app installation. This demonstrates that it is possible to develop an app that is popular, functional and privacy-friendly.

私隱專員評論

- 流動裝置已改變了商業運作及我們的生活，裝置內往往載有大量個人資料，包括許多生活上的個人私隱，使用這些裝置時，私隱保障變得非常重要。
- 抽查應用程式結果清楚顯示本地流動應用程式的私隱政策透明度，明顯不足，強差人意。
- 要尊重用戶的私隱，透明而公開的政策是必須的。程式要求查閱大量個人資料，卻未有充分解釋會如何收集、使用及披露個人資料，用戶下載具私隱風險；程式開發商在保障使用流動裝置的私隱事宜中，責無旁貸。

公署加強的執法及推廣工作

本地行動

- 保障使用流動裝置私隱是公署2014及2015年的私隱保障的重要工作，公署會強與業界的聯繫及公眾的教育，以確保各方均嚴謹看待私隱保障。
- 公署於2014年初起已舉辦了八場的程式開發須知研討會，協助他們了解及要求他們遵從條例訂定的法律責任。
- 於2014年11月25日出版《開發流動應用程式最佳行事方式指引》，以簡易的指引協助程式開發商有效地為程式設計進行私隱風險評估。
- 為遏止違規情況繼續擴散，及增加阻嚇力，公署會嚴肅調查投訴的個案，並主動開展符規調查，繼而採取執法行動。

國際聯合行動

- 電子世界中參與收集及使用個人資料的持份者亦擔當私隱保障的重要角色；包括裝置生產商及應用程式供應平台（Google Play和Apple App Store等）。
- 世界各地的私隱執法機關在2014年12月9日發出公開信，促請應用程式供應平台強制規定，若流動應用程式開發商要收集個人資料，必須在用戶下載程式前提供私隱政策連結，讓用戶清楚明白應用程式如何收集、使用及披露其個人資料以決定下載與否。
- 公開信由香港個人資料私隱專員公署與加拿大私隱專員公署聯合發起，其他21個資料保障機關已簽署支持。
- 公署相信應用程式供應平台若承諾要求平台上的所有應用程式及時向用戶提供有關查閱或收集個人資料的私隱政策，便可發揮重要的把關角色。

The Commissioner's Comments

- Mobile devices are ubiquitous and have transformed business operations and our lives. With all they contain and all they may reveal, they hold for many people the privacies of life. Safeguarding privacy in the use of these devices is therefore imperative.
- The findings reveal prevalent inadequacies in the transparency of privacy policies of local apps.
- Transparency is central to respecting the privacy of individuals and it is paramount that organisations develop transparent online privacy policies. Apps request access to a wide range of personal data without explaining how the data would be collected, used and disclosed, putting users' privacy at risk. App developers must live up to the responsibility of safeguarding privacy in the use of mobile devices.

PCPD's Enhanced Enforcement and Promotion Work

Local initiatives

- Safeguarding privacy in the use of mobile devices is the PCPD's prime objective in 2014 and 2015. The PCPD will continue to engage the app developers' community and the general public to ensure that they do take privacy seriously.
- The PCPD has conducted a total of eight seminars with mobile app developers in 2014 to assist them in understanding and complying with the Ordinance.
- The PCPD published on 25 November 2014 "Best Practice Guide for Mobile App Development", a simple and handy guide for app developers to conduct privacy risk assessment when designing apps.
- To deter proliferation of the malpractices, the PCPD will investigate into complaints and initiate compliance investigations, and take appropriate enforcement actions.

Cooperation with overseas regulators

- Not only the organisations collecting data directly but also device or operating system manufacturers and app marketplaces play an important role in safeguarding consumer privacy.
- On 9 December 2014, privacy enforcement authorities from around the world called on (in an open letter) app marketplaces to make it mandatory for mobile app developers to post links to privacy policies prior to download if they are going to collect personal information. Having such information about privacy policies allows individuals to decide prior to download whether they are comfortable with the collection, use and disclosure of their personal data before the app is even on their device.
- The open letter was initiated jointly by the PCPD and the Office of the Privacy Commissioner of Canada. 21 other data protection authorities have signed on in support.
- The PCPD believes the app marketplace operators play an important gatekeeping role if they commit to require all apps under their listings to provide users with timely access to the app's privacy policy concerning access or collection of personal data.

私隱專員發現 Android 的權限模式有缺陷
The Commissioner Uncovered Privacy Failure in Android's Permission Model

在抽查本地流動應用程式期間，公署發現 Android 程式可以被編寫至在未有作出權限聲明的情況下，讀取 Android 4.3 或之前版本的流動裝置的公共記憶體。

Android 一直以來的運作模式是，程式要讀取的資料會在安裝程式前呈現在「權限」頁面 ，若沒有呈現即不能被讀取。然而，公署的測試揭示，程式有機會在毋須於權限頁面作有關聲明的情況下，仍可讀取 Android 裝置內的記憶體內容，包括相片、檔案及其他程式儲存在該記憶體的資料。雖然有關可以讀取公共記憶體的缺陷已在 Android 4.4 的裝置糾正，但可以讀取部分內部記憶體的情況仍有可能於 Android 4.4 發生，故此情況依然值得關注。再者，目前有三分之二的 Android 用戶仍在使用 Android 4.3 或更舊的版本 ，當中部份裝置更無法更新至 Android 4.4。

公署自本年 8 月已聯絡 Google，證實這缺陷的存在。公署於 2014 年 11 月 27 日正式要求 Google 採取補救措施，及/ 或警告受影響的用戶惡意程式可以在其不知情甚至不允許的情況下讀取資料而存在風險。

為了作出補救，公署建議程式開發商把儲存在流動裝置公共記憶體的資料加密，以避免未經授權的讀取或資料外洩。公署亦建議消費者考慮把儲存在流動裝置的敏感資料加密 。

During the Sweep exercise, the PCPD had discovered that it is possible for an Android app to read the shared memory in a mobile device running on Android 4.3 or earlier versions without the need to make a prior declaration on permission.

Android had all along worked on the model that, prior to app installation, all intended access to data stored in an Android device would be fully disclosed on the Permission Page. Otherwise, no data can be accessed. However, PCPD's tests have revealed that it is possible to develop an app that can read the memory of Android devices, including photos, files, and any data other apps choose to store in the devices, without the need to inform app users on the Permission Page. Although the flaw has been corrected for Android 4.4 for access to the shared memory, it is still a cause for grave concern as partial access to the internal memory without prior declaration is still possible for Android 4.4. Furthermore two-thirds of Android users are still using devices running on earlier versions of the platform and some of these devices could not be upgraded to Android 4.4.

The PCPD had contacted Google Inc. since August 2014 and confirmed with them the existence of the flaw. Google Inc. was formally requested on 27 November 2014 to take corrective action and/or warn the end-users concerned that they are subject to the risk of data access by malicious apps without their knowledge and permission.

As a means to remedy the problem, PCPD advises app developers to encrypt data they store in the shared memory of mobile devices to guard against unauthorised access or leakage. The PCPD further advises consumers that if they need to consider storing sensitive information in the mobile devices, protection by encryption is recommended.

個案：香港航空旅遊有限公司不慎使用流動應用程式「俠客行．旅行」外洩個人資料
Case: Personal Data Leaked through Inadvertent Use of Mobile Application "TravelBud" by HKA Holidays

公署的調查報告指，香港航空旅遊有限公司（「港航旅遊」）於 iOS 平台運行的流動應用程式「俠客行．旅行」（「俠客行」）外洩顧客的個人資料，原因是其程式保養承辦商佰邦達科技（北京）有限公司（「佰邦達」）沒有就 iOS7 推出新增保障私隱的功能（阻止程式讀取 MAC 位址[1] 作為識別流動裝置），及時作出相應行動。而作為資料使用者的港航旅遊，違反了條例附表一保障資料第 4(1) 原則。

俠客行是一個旅遊助理的應用程式，為流動裝置用戶提供預訂及購買機票等在線服務會員及非會員首次使用預訂服務時，均須輸入乘客的個人資料（全名、性別、出生日期、身份證或護照號碼）及聯絡人的個人資料（姓名、電話號碼及電郵地址）。當非會員再次進行交易時，俠客行會以其流動裝置的 MAC 位址確認其身份。

2013 年 9 月 18 日（美國時間），蘋果公司推出新的流動操作系統 iOS7。以保護私隱為由，iOS7 阻止所有應用程式讀取 MAC 位址作為識別流動裝置的持有人。在回應應用程式要求讀取 MAC 位址時，iOS7 會向程式提供一組固定數

字，而不是披露真正的MAC位址。

由於佰邦達沒有就該改動採取任何相應的調整，於2013年9月19日起（香港時間），每當非會員在iOS7版本的流動裝置進行交易時，iOS7均會以相同的虛假MAC位址回應，所有交易均因此被視為由同一個人作出。當非會員以運行iOS7版本的流動裝置預訂機票或查詢訂購紀錄時，俠客行在裝置的螢幕上不單顯示他的紀錄（訂購紀錄及個人資料），還會顯示其他非會員（同樣使用運行iOS7版本的流動裝置）的個人資料。直至事件於2013年9月25日被揭發為止，共有六名顧客的個人資料因這方式而外洩予其他非會員。

An investigation report of the PCPD revealed the leakage of personal data of the customers of an airline services company, HKA Holidays Limited ("HKA Holidays") through "TravelBud" , a mobile application ("app") running on iOS platform. This stems from the failure of the app maintenance contractor, BBDTEK Company ("BBDTek"), in responding to the new privacy protection feature of iOS7 which blocked the reading by apps of MAC address[1] as a device identifier. HKA Holidays as the data user has contravened Data Protection Principle ("DPP") 4(1) in Schedule 1 to Ordinance.

TravelBud is a travel assistant app providing online services to mobile device users such as flight ticket reservation and purchase. For reservations for the first time, both members and casual customers had to input the passenger's personal data (full name, gender, date of birth, identity card number or passport number) and a contact person's personal data (name, telephone number and email address). For subsequent transactions, casual customers were recognised by the MAC address of the mobile device with the app installed.

On 18 September 2013 (US time), Apple Inc. launched its new mobile operating system iOS7 which, for reason of privacy protection, would block the reading by apps of MAC address as a mobile device identifier. In response to apps asking for the MAC address, iOS7 would provide a fixed number instead of disclosing the true MAC address.

As BBDTek took no adjustment action to this change of MAC address behaviour, all casual customers making transactions under iOS7 from 19 September 2013 (Hong Kong time) onwards were identified as one person based on the same fictitious MAC address. As a result, in response to a casual customer attempting to reserve or purchase a flight ticket or make an order history enquiry using a mobile device operating on iOS7, TravelBud would show on the screen of the mobile device not only his records (order histories and personal data) but also those of all other casual customers who had made transactions through TravelBud under iOS7. There were six affected customers whose personal data was leaked to other non-members in this way before the incident was identified on 25 September 2013.

佰邦達是否已適時回應 iOS 7 會帶來的轉變
Whether BBDTek had promptly responded to the change in the operating environment of mobile devices

佰邦達的解釋 **BBDTek's Defence**	公署意見 **PCPD's Comments**
• 在2013年9月11日之前一直未知悉蘋果公司發出任何有關流動操作系統變更或更新的通知或消息 • 直至蘋果公司於2013年9月11日對外公告iOS7將於2013年9月18日正式推出，他們才首次獲得有關資訊 • 他們在2013年9月才登記參與iOS開發商計劃，錯過了蘋果公司較早前給予其已登記的程式開發商有關推出iOS7的電郵通知 • It was unaware of Apple Inc.'s notification or news in relation to the changes or updates of the mobile operating system until 11 September 2013. • It only registered with the iOS Developer Program in September 2013 and would not have received relevant email notification from Apple Inc.	• 佰邦達應緊貼蘋果公司的消息及最新科技資訊 • 蘋果公司已就iOS7推出時間及有關MAC位址的變更向程式開發商給予充足的通知。佰邦達作為專門從事程式開發的科技公司，這不知情的解釋令人難以置信 • 即使如此，佰邦達仍有足夠時間（由該日至iOS7正式推出尚有一星期）採取行動，更新程式以防資料外洩 • BBDTek should have kept abreast of the news and technology updates from Apple Inc. • Apple Inc. had given ample notice to all app developers of when iOS7 would be introduced and what the changes in relation to MAC address were. It is inconceivable that BBDTek, as a technology company specialising in app development, was unaware of Apple Inc.'s notification or news. • iOS7 was launched a week later on 18 September 2013, there was still time for BBDTek to take steps to prevent the data breach.

1. 媒體存取控制位址（"MAC位址"）是編配予網絡裝置的獨一無二的識別碼，以促成網絡裝置通訊之用。此位址通常由網絡裝置製造商編配，而存在於所有流動電腦裝置例如智能電話中。

   A media access control address ("MAC address") is a unique identifier assigned to a network device to facilitate its communications in the network. It is assigned by the manufacturer of a network device and exists on all mobile computing devices such as a smartphone.

私隱專員評論

- 佰邦達未能應對MAC位址操作模式的變更，是導致是次資料外洩的主因，責無旁貸。但由於佰邦達只是港航旅遊的外判代理，亦沒有涉及處理顧客的個人資料，所以不屬條例下的資料使用者。私隱專員不能對其直接採取執法行動。
- 根據條例第65(2)條，港航旅遊作為委托人須為佰邦達的錯失負責。因此，私隱專員認為港航旅遊違反保障資料第4(1)原則的規定。
- 2013年10月1日，港航旅遊發出在iOS平台運作的俠客行更新版本，作出了下述補救措施：
  - » 不再以MAC位址識別非會員身份
  - » 停止非會員查詢訂單的功能
  - » 非會員只可購買機票，而在每次購買時均須重新提供乘客及聯絡人的個人資料
- 港航旅遊已作出足夠的補救措施，而俠客行的法律擁有權已於2014年1月轉移予一內地公司。 基於這些情況，私隱專員未有向港航旅遊送達執行通知。
- 不過，私隱專員已向港航旅遊作出警告，如日後在類似情況中沒有遵守條例的相關規定，私隱專員會考慮對其採取執法行動。
- 雖然大部份的程式開發商如「佰邦達」屬中小型企業，但仍有責任要遵從條例的規定。他們必須要與時並進，緊貼最新的科技發展及趨勢，在更新其開發的流動應用程式並改進有關功能時，確保不會影響私隱及資料的保障。
- 當機構外判程式的開發時，應小心揀選信譽好及在私隱保障勝任的程式開發商。
- 如聘用外判代理時沒有採取妥善的措施，導致個人資料一旦因代理的疏忽而外洩或遭濫用，可能會對其顧客造成嚴重傷害並有損商譽。
- 機構監督應用程式開發商，可參考詳列於是次調查報告及公署的「外判個人資料的處理予資料處理者」資料單張(www.pcpd.org.hk/tc_chi/resources_centre/publications/information_leaflet/files/dataprocessors_c.pdf)中所建議的合約條款。

調查報告：www.pcpd.org.hk/tc_chi/enforcement/commissioners_findings/investigation_reports/files/R14_6453_c.pdf

The Commissioner's Comments

- BBDTek failed to respond to the change of MAC address behaviour, thus causing the leakage incident. However, BBDTek was only an outsourced agent of HKA Holidays and was not provided or entrusted with any personal data of the latter's customers for processing. Accordingly, BBDTek was not a data user as defined under the Ordinance. Therefore, the Commissioner cannot take direct enforcement action against it.
- By virtue of section 65(2) of the Ordinance, HKA Holidays as BBDTek's principal was responsible for BBDTek's misdeed.
- On 1 October 2013, HKA Holidays released an updated version of TravelBud for running on iOS platform, which had the following remedial features: -
  - » MAC address was no longer used to identify non-members
  - » The order history enquiry function for non-members was disabled
  - » Non-members could still purchase flight tickets but needed to provide personal data of passengers and contact persons for each purchase
- The Commissioner considers that HKA Holidays has taken adequate steps to remedy the contravention. On the other hand, the legal ownership of TravelBud was transferred from HKA Holidays to a Mainland company. In the circumstances, no enforcement notice has been served on HKA Holidays.
- Instead, the Commissioner has warned HKA Holidays that enforcement action would be taken should it fail to observe the relevant requirements under the Ordinance in similar situations in future.
- Although most app developers are mostly small and medium enterprises, they still have the obligation to comply with the requirements under the Ordinance. It is incumbent upon them to keep abreast of the relevant trends and developments in technology so that they can update the apps they have developed to achieve enhanced functionality without compromising privacy and data protection.
- When outsourcing the development of the apps, an organisation should exercise care and choose competent app developers with good track records. Without appropriate safeguards in appointing outsourced agents, leakage or misuse of the personal data due to the agents' negligence might happen, thus causing serious harm to its customers and bringing the organisation into disrepute.
- An organisation may consider adopting the recommended contractual terms found in the investigation report and in PCPD's "Outsourcing the Processing of Personal Data to Data Processors" information leaflet (www.pcpd.org.hk/english/resources_centre/publications/information_leaflet/files/dataprocessors_e.pdf).

Investigation Report: www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R14_6453_e.pdf

個案：翱翔旅遊的流動應用程式未有提供私隱政策並收集過度個人資料

Case: Excessive Collection of Personal Data through Mobile Application by Worldwide Package Travel Service Operating with No Privacy Policy

公署另一份調查報告指，翱翔旅遊有限公司（「翱翔遊」）在顧客 (i) 參加客戶獎賞計劃「翱翔天地」（「該計劃」）及 (ii) 於流動應用程式（「該程式」）查詢該計劃的積分時，收集過量的個人資料。該程式由縱橫旅遊有限公司（「縱橫遊」）開發及由翱翔遊營運。另外，翱翔遊和縱橫遊兩間公司均沒有透過私隱政策、應用程式供應平台上的敘述或其他溝通渠道，向該程式的用戶解釋收集資料的用途。兩間公司均違反了條例附表一保障資料第 1 原則。

縱橫遊是一間批發旅遊產品的本地旅行社，翱翔遊是縱橫遊的指定銷售代理。該計劃是由翱翔遊獨自管理。顧客購買旅遊產品後，可以加入成為該計劃會員。顧客填寫申請表格時要提供姓出生日期及身份證號碼等個人資料，不過在三萬名登記會員中，約有二千人沒有提供出生日期，三千人沒有提供身份證號碼，但申請仍然被翱翔遊接納。申請經接受後，顧客會獲發一個會員編號。

The PCPD published another investigation report concerning the excessive collection of personal data by Worldwide Package Travel Service Limited ("Worldwide Travel") from customers when they enrolled for the company's loyalty programme ("Programme") and when making online enquiries about the reward points under the Programme using the mobile application ("App") developed by Package Tours (Hong Kong) Limited ("Package Tours") and operated by Worldwide Travel. Further, both Worldwide Travel and Package Tours did not explain to the App users the purpose of use of the customers' personal data they collected via a privacy policy, app marketplace description or other communication means. The two companies have contravened the Data Protection Principle ("DPP") 1 in Schedule 1 to the Ordinance.

Package Tours is a local travel agent providing wholesale travel products and Worldwide Travel is its designated sales agent. The Programme is exclusively administered by Worldwide Travel. Customers after having made a purchase of the company's travel products may join the Programme. In completing the Programme application form, the customer supplies his personal data including date of birth ("DOB") and identity ("ID") number. There were about 30,000 registered members under the Programme. Of these, around 2,000 and 3,000 members did not provide their DOB and ID number respectively but Worldwide Travel still accepted the application. Upon enrolment, the customer is assigned a membership number.

收集過度的個人資料：「翱翔天地」
Excessive Collection of Personal Data – the Programme

過度收集的個人資料 **Personal Data Excessively Collected**	出生日期及身份證號碼 DOB and ID Number
資料使用者 **Data User**	翱翔遊 – 獨自營運及管理「翱翔天地」，以及其電腦系統及資料庫 Worldwide Travel who solely manages and operates the Programme
翱翔遊聲稱的收集目的 **Collection Purpose Stated by Worldwide Travel**	為提供服務時（包括會員查詢其帳戶資料、查詢／換取積分），核實會員身份 To identify the applicants/members when providing services under the Programme

公署觀察資料
PCPD's Observations

- 即使申請人沒有在申請表提供出生日期或身份證號碼，翱翔遊仍然接納其申請
- 會員親身及致電熱線查詢時，只須提供會員編號、姓名、電郵地址及／或流動電話號碼，亦足以辨識其身份
- 出生日期及身份證號碼在「翱翔天地」的電腦系統中並非會員資料的搜尋準則
- 2013 年 5 月修訂申請表，取消收集身份證號碼，但卻沒有落實生效日期，並容許分行繼續使用舊申請表：可能繼續超乎適度地收集身份證號碼
- Worldwide Travel accepted the application when the applicants did not provide their DOB or ID number on the application forms.
- For in-person and hotline enquiry, a member's membership number or his name, email address and/or mobile phone number would suffice for identification.
- DOB and ID number are not made search criteria in the computer system for the Programme.
- Worldwide Package revised the application form and stopped collecting applicants' ID Number in May 2013, but it did not specify an effective date for the new form and allowed the old forms to be used until stock depletion. This may lead to prolonged excessive collection of ID number.

收集過度的會員個人資料：「積分查詢」功能
Excessive Collection of Personal Data - "Reward Points Enquiry" Function

過度收集個人資料 **Personal Data Excessively Collected**	出生日期及身份證號碼 DOB and ID Number
資料使用者 **Data User**	翱翔遊 (1) 負責處理「縱橫遊」程式收集的個人資料 (2) 程式是在翱翔遊操作的電腦系統及伺服器中運作 Worldwide Travel who is responsible for the collection and processing of personal data through the App, and the App operates on the computer system and servers of the Programme run by Worldwide Package.
翱翔遊聲稱的收集目的 **Collection Purpose Stated by Worldwide Travel**	核實會員身份 To verify a member's identity

公署觀察資料
PCPD's Observations

- 翱翔遊實際上（親身及熱線查詢）只需使用私隱敏感度較低的個人資料（例如姓名及聯絡資料），便能可靠地核實會員身份
- 雖然每名會員都獲編配會員編號，以辨識會員身份，但用戶介面卻沒有欄目以輸入會員編號
- 查詢積分餘額是相對較不重要的事，收集出生日期及身份證號碼以核實會員身份的做法屬不必要及超乎適度
- For in-person and hotline enquiry, Worldwide Package was able to authenticate reliably the identity of a member by merely using less sensitive personal data, such as his name and contact information.
- Membership number was not made a data field in the customer interface under the App notwithstanding a member is always able to check his account through in-person or hotline enquiries by just quoting his membership number.
- Enquiry about reward points balance was a relatively inconsequential matter, collection of DOB and ID was unnecessary and excessive.

透過「縱橫遊」程式收集個人資料：沒有提供通知
Failure to Provide Notification to App users

功能 **Function**	資料使用者 **Data User**	
網上訂購 Online Purchase	翱翔遊及縱橫遊 Worldwide Travel and Package Tours	• 處理銷售旅遊產品時，共用同一個電腦系統及資料庫 • 翱翔遊負責接收及確認程式發送的網上訂單 • 縱橫遊負責向航空公司購買機票及團體旅遊保險 • Both Worldwide Travel and Package Tours share the same database and computer system for managing the sale of the travel products. • Worldwide Travel is responsible for receiving and acknowledging online purchase orders made through mobile devices via the App. • Package Tours is responsible for flight tickets issuance with airlines and purchase of group travel insurance.
積分查詢 Reward Points Enquiry	翱翔遊 Worldwide Travel	見上表「積分查詢」功能 See the table above "Reward Points Enquiry" Function

公署觀察資料
PCPD's Observations

「網上訂購」及「積分查詢」功能均會收集個人資料，但卻沒有提供以下資訊：-

- 收集個人資料的目的
- 資料承轉人的類別
- 用戶要求查閱及改正資料的權利
- 處理查閱及改正資料要求的人士的姓名或職銜及地址

Both functions collect personal data but do not provide the following information: -

- the purpose for which the data is to be collected
- the classes of persons to whom the data may be transferred
- user's right to request access to and correction of the data
- the name or job title, and address, of the individual who is to handle any such request.

調查結果
Contraventions by Package Tours and Worldwide Package

違反相關的保障資料原則及說明 **Contravention of the relevant DPPs and description**		縱橫遊 **Package Tours**	翱翔遊 **Worldwide Package**
保障資料第 1(1) 原則 DPP1(1)	「翱翔天地」的申請過程過度收集申請人的出生日期及身份證號碼 Excessive collection of DOB and ID number for verifying members' identity during Programme application	不適用 N/A	✔
	應用程式「積分查詢」功能過度收集會員的出生日期及身份證號碼 Excessive collection of DOB and ID number through Reward Points Enquiry under the App		
保障資料第 1(3)(b) 原則 DPP1(3)(b)	應用程式「網上訂購」功能沒有通知程式用戶相關資訊 Failed to inform the users of the relevant information during Online Purchase on the App	✔	✔
	應用程式「積分查詢」功能沒有通知程式用戶相關資訊 Failed to inform the users of the relevant information during Reward Points Enquiry on the App	不適用 N/A	

私隱專員評論

- 送達執行通知，指令翱翔遊在21日內：–
  - » 停止向參加「翱翔天地」的申請人收集出生日期及身份證號碼
  - » 停止使用「翱翔天地」於2013年5月之前採納的申請表，並進一步修訂新的表格，以刪除提供出生日期的要求，並即時落實使用修訂表格
  - » 停止透過「積分查詢」功能收集出生日期及身份證號碼
  - » 完全刪除在「翱翔天地」所收集的出生日期及身份證號碼
  - » 聯同縱橫遊在「縱橫遊」程式根據保障資料第1(3)(b)原則的規定提供《收集個人資料聲明》
- 送達執行通知，指令縱橫遊在21日內：–
  - » 聯同翱翔遊在「縱橫遊」程式根據保障資料第1(3)(b)原則的規定提供《收集個人資料聲明》
- 個案印證公署於2013及2014年抽查應用程式帶出的憂慮，顯示本地流動應用程式的私隱政策透明度明顯不足。「縱橫遊」開發及由「翱翔遊」營運的「網上訂購」及「積分查詢」程式正是一例子，用戶不能掌握資料會用於甚麼目的及該資料可能轉移予甚麼類別的人。
- 向程式用戶提供私隱資訊殊不容易，因為流動裝置螢幕細小，用戶多數不會專注閱讀。然而，遵從條例是必然的法律責任。
- 抽查結果亦顯示大部分程式要求讀取資料的權限似乎超越該程式功能的實際需要。「翱翔遊」正是過度收集資料，而忽略評估收集每項資料的真正需要。
- 機構有需要廣泛採用應用程式，利用科技和創意尋找營商之道及增強競爭力，以吸引更多客戶。即使技術不太成熟的機構也知道流動應用程式的價值，包括提高它們在市場的知名度以至收集大量個人資料。
- 倉猝推出這些程式的過程中，機構未必充分了解私隱風險或管理，及投放足夠資源以識辨或解決有關問題。因此，我們看到初涉足數碼世界的機構新手所犯的毛病越多。
- 擔憂本報告揭示「縱橫遊」及「翱翔遊」的不當行為，可能只是冰山一角。
- 呼籲機構以客為本，應用程式可接觸無數的顧客、客戶和用家。要尊重用戶的私隱，透明而公開的政策是必須的。若能有效地保障顧客私隱，可以贏取他們的信任，建立忠誠的關係，這正是成功營商的基石。

調查報告：www.pcpd.org.hk/tc_chi/enforcement/commissioners_findings/investigation_reports/files/R14_9945_c.pdf

The Commissioner's Comments

- The Commissioner has served an enforcement notice on Worldwide Travel directing: -
  - » Worldwide Package to cease collection of DOB and ID number from applicants for joining the Programme
  - » Worldwide Package to cease to use the Form adopted prior to May 2013 and to further revise the new Form for immediate implementation by deleting the requirement of provision of DOB
  - » Worldwide Package to cease the collection of DOB and ID number through the Reward Points Enquiry function under the App;
  - » Worldwide Package to completely delete from the Programme the DOB and ID number collected; and
  - » Package Tours and Worldwide Package to provide a "Personal Information Collection Statement" in the App in the manner prescribed under DPP1(3)(b)
- The case proved the privacy concern brought by the PCPD surveys in 2013 and 2014 which revealed that transparency in terms of privacy policy of local mobile apps was clearly inadequate. The App developed by Package Tours (Hong Kong) Limited and operated by Worldwide Package Travel Service Limited is an example. User is not able to understand how their data will be used and to whom the data will be transferred.
- Conveying privacy information to consumers can present unique challenges in the app world, where screens are small and users' attention can be intermittent. That said, compliance with the legal obligations under Ordinance is a must.
- The survey also found that the most of the apps seemed to have sought permissions for data access beyond what was actually required based on the app's functionality. Worldwide Travel collected excessive personal data without assessing the genuine need for collecting individual data items.
- App revolution is a prime example of the use of technology and innovation to reinvent competitive solutions and business models. Almost every organisation wants an app to drive more consumer traffic. Even organisations that are relatively green in technological maturity understand the value an app can provide, from enhancing their appeal in the market to collecting enormous amounts of personal data.
- In a rush to adopt apps, they may not know enough about privacy risks or management and devote adequate resources to either identify or address them. As a result, we are seeing an increasing number of rookie mistakes made by organisations as they step into the digital world.
- The malpractice by Package Tours (Hong Kong) Limited and operated by Worldwide Package Travel Service Limited may represent merely the tip of the iceberg.
- A customer-focused organisation will appreciate that an app provides an interface between the organisation and potentially millions of customers, clients and users. The Commissioner strongly advocates that privacy policies must be effectively communicated. Transparency is central to respecting the privacy of individuals and will be rewarded with customer trust and loyalty: the cornerstone of business success.

Investigation Report：www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R14_9945_e.pdf

私隱專員促請當局把人對人直銷電話納入拒收訊息登記冊
The Commissioner Urges the Administration to Expand the Do-not-call Registers to Include Person-to-person Calls

私隱專員委託香港大學社會科學研究中心於 2014 年 3 月就人對人直銷電話進行公眾意見調查，並把調查結果與通訊事務管理局辦公室（「通訊辦」）於 2008 年進行的同類調查相比，結果顯示人對人直銷電話的數量再趨上升，更多人表示對這類電話反感，而從這類電話中得益的不單只佔非常少數，更有下降趨勢。調查結果支持私隱專員向當局提出擴大拒收訊息登記冊的建議。

現時由通訊辦的拒收訊息登記冊，讓電話用戶登記其電話號碼，拒絕接收非應邀商業電子訊息，包括傳真、短訊和預先錄製電話訊息，但不包括人對人電話。

人對人直銷電話的調查

私隱專員在 2014 年 8 月 5 日舉行記者會，公佈有關調查結果。消費者委員會（「消委會」）亦歡迎私隱專員就消費者對於「人對人促銷電話」的意見作研究；並表示近年利用「電話促銷」來開拓市場已非常普遍，相關手法的應用更呈顯著上升，議題值得關注。消委會表示消費者的意見調查一方面提供了客觀的數據和具體的分析，另一方面也可以檢視市場趨勢，增加機構對議題的理解，進一步保障消費者權益。

私隱專員提醒機構，法律規定機構在直接促銷中首次使用個人資料時，必須告知該名人士有拒收訊息的權利。該名人士亦可以隨時行使這項權利。若顧客已提出這要求，機構必須停止使用其個人資料作直接促銷。

The Commissioner commissioned the Social Sciences Research Centre of The University of Hong Kong to conduct a public opinion survey in March 2014 on person-to-person direct marketing calls ("P2P calls"). Compared to a similar survey conducted by the Office of the Communications Authority ("OFCA") in 2008, the 2014 survey revealed that there was a growing preponderance of P2P calls, with more people responding negatively to the calls and fewer people reporting anything positive about the calls. The findings supported the appeal to the Administration to expand the Do-not-call ("DNC") registers .

The DNC registers, currently administered by the OFCA, provide for telephone subscribers to register their telephone numbers to ward off unsolicited commercial electronic messages, which include, at present, fax messages, short messages and pre-recorded telephone messages, but exclude person-to-person calls.

Survey on person-to-person direct marketing calls

The Commissioner announced the results of the survey at a press conference on 5 August 2014. The Consumer Council welcomed the PCPD's efforts to understand consumer attitudes towards person-to-person direct marketing calls, and opined that the results of the survey would enhance understanding and monitoring of market trends, providing useful information and data for concrete analysis of the issue. The Consumer Council pointed out that these findings and analysis were valuable for the protection of consumer rights.

The Commissioner pointed out that it is a legal requirement for companies to notify customers of their opt-out right when using their personal data in direct marketing for the first time. Thereafter, the customers may exercise this right at any time, and, in response, the company must then cease to use their data for direct marketing.

調查摘要：
www.pcpd.org.hk/tc_chi/resources_centre/publications/surveys/files/p2p_survey_sum_c.pdf

調查報告全文（只有英文）：
The full survey report (with executive summary):
www.pcpd.org.hk/english/resources_centre/publications/surveys/files/p2p_survey_e.pdf

2014 年 8 月 21 日專員網誌「人對人直銷電話的拒收訊息登記冊 最終由哪一個政策局負責？」全文：
www.pcpd.org.hk/tc_chi/about_pcpd/commissioners_message/blog_21082014.html
The Commissioner's Blog on 21 August 2014 – Renewed Call to Set Up a Do-not-call Register for Person-to-person Telemarketing Calls caught between two Bureaux":
www.pcpd.org.hk/english/about_pcpd/commissioners_message/blog_21082014.html

有問有答：人對人直銷電話
Questions and Answers: Person-to-person ("P2P") Telemarketing Calls

問 1：2014 的數字怎樣與 2008 年的數字作比較？

答 1：數字反映人對人直銷電話的數量再趨上升，更多人表示對這類電話反感：

	2008	2014
曾接收人對人直銷電話的受訪者	84%	91%
估計每星期收到六個或以上電話的受訪者	8%	23%
以「對來電者表明無興趣」來回應人對人直銷電話的受訪者	43%	49%
會「先聆聽資訊再決定是否有興趣」的受訪者	46%	28%
不聆聽資訊便立即中斷電話的受訪者	11%（最多）	21%
表示人對人直銷電話構成不便的受訪者	81%	81%
表示人對人直銷電話帶來不便的受訪者，其中進一步指這些電話構成滋擾[1]	–	99%

問 2：但這些電話肯定會為某些人帶來一些好處？

答 2：2014 年的數字顯示更少人從人對人直銷電話中得到好處：

	2008	2014
從一些人對人直銷電話中得到好處的受訪者	13%	6%
在一些電話中有作出商業交易的受訪者	21%	16%

問 3：2014 年的數字在統計上是否可靠？

答 3：大部分上述提及的數字均是可靠的；今次 2014 年的調查，與通訊辦在 2008 年的調查，是由同一研究中心進行。詳細報告可在 www.pcpd.org.hk/english/resources_centre/publications/surveys/files/p2p_survey_e.pdf 下載，當中亦包括了比較 2008 年與 2014 年兩次調查結果差異的顯著性檢定測試。調查結果顯示了無可置疑的大圖畫：這類電話只為相對一少撮的消費者帶來或多或少的得益，但卻要大多數人忍受滋擾，而且這趨勢正在轉得熾熱。

問 4：加強監管人對人直銷電話會否影響數以萬計直銷電話業務從業員的生計？

答 4：維持現狀的代價是要對大多數人造成不便和滋擾，這與新加坡於 2014 年初設立拒收訊息登記冊（包括人對人直銷電話、短訊和傳真）的做法背道而馳；新加坡為使國內經濟工作增值，其政府並不介意減少價值較低的電話直銷活動。若香港仿效類似做法，可以設立適度的過渡期，來紓緩就業減少的憂慮。登記冊甚至可以按直銷產品/服務的行業來逐步實施，而不是「一刀切」全面實施。當局亦可以向受影響僱員提供協助，幫他們提升技能，進而從事較高增值的工作。

問 5：金融服務業、保險業、電訊業及直銷電話中心的自我規管是否足以減少對公眾造成的滋擾？

答 5：現時並沒有強制規定電話促銷商須加入這些行業的聯會，遵守由這些聯會制定的守則亦屬自願性質。

問 6：設立拒收人對人直銷電話登記冊的建議未必可有效地打擊從香港境外打來的電話，尤其是當電話不涉及使用個人資料。

答 6：值得考慮的建議是，由本地直銷電話行業建立認證制度，以提高業界的專業水平。獲認證的直銷中心可向政府當局爭取使用經認可的、獨有的四位數字字頭電話號碼，與未獲認證的直銷中心（包括在境外操作的）區分開來。

問 7：2013 年的條例修訂對直銷活動的規管是否足以阻止不必要的人對人直銷電話？

答 7：條例只適用於涉及使用個人資料的電話。2014 年的調查報告顯示，只有 27% 受訪者表示接到的人對人直銷電話中，過半數可稱呼他們的名字，反映人對人直銷電話的問題源頭主要是來自不涉及使用個人資料的「冷電」(Cold Call)。設立拒收人對人直銷電話登記冊的建議優點是能涵蓋所有來電，包括隨機抽打出的電話而不涉及個人資料。再者，根據條例，消費者不論同意收取或其後拒絕繼續接收直銷訊息，都須向個別公司逐一提出。相比之下，拒收訊息登記冊可提供一站式服務，消費者從一開始便可一次過拒絕所有不願接收的直銷電話。條例的規管與設立拒收人對人直銷電話登記冊，有互補功效。

問 8：人對人直銷電話登記冊附設於由通訊辦監管的《非應邀電子訊息條例》，還是於由公署監管的條例會比較可行？

答 8：前者會比較簡單。《非應邀電子訊息條例》現行的寫法，是方便日後若決定把人對人直銷電話納入其規管範圍，只需依據該條例第 7 條，在憲報刊登公告，便可迅速生效。此外，現時通訊辦已在管理拒絕接收短訊、預先錄製電話訊息和傳真訊息的登記冊，擴大有關登記冊的涵蓋範圍至人對人電話，在行政上也較為方便。如果由公署加設管理拒收人對人直銷電話登記冊是架床疊屋，實在不利有效地運用公共資源，亦使消費者感到混亂及不便。

Q1: How do the 2014 figures compare with the 2008 figures?

A1: They show a growing preponderance of the calls, with more people responding negatively to the calls:

	2008	2014
Proportion of respondents receiving calls	84%	91%
Frequency of calls as assessed by proportion of respondents receiving 6 or more calls per week	8%	23%
Proportion of respondents indicating to the caller they were not interested	43%	49%
Proportion of respondents who would listen to the caller before deciding if they were interested	46%	28%
Proportion of respondents who would discontinue the call without listening to the caller	11% (at most)	21%
Proportion of respondents reporting that the calls had caused inconvenience to them	81%	81%
Proportion of respondents reporting inconvenience who considered the calls had caused nuisance to them[1]	–	99%

Q2: But surely the calls must have brought some benefits to some people?

A2: The 2014 figures show fewer people reported gains from the calls:

	2008	2014
Proportion of respondents who had derived benefits from some (not all) of the calls	13%	6%
Proportion of respondents who had concluded commercial transactions during some (not all) of the calls	21%	16%

Q3: Are the 2014 figures statistically valid?

A3: Yes, for most of the figures quoted above. The researcher the PCPD commissioned to undertake the 2014 survey was the same researcher who undertook the 2008 survey. The statistical testing of the 2014 survey results and the difference between the 2008 and 2014 results are found in the full report at www.pcpd.org.hk/english/resources_centre/publications/surveys/files/p2p_survey_e.pdf. The broad picture revealed by the survey results is indisputable, namely, while the P2P calls have successfully brought benefits to a relatively small proportion of the population, the majority has been caused nuisance and the trend is worsening.

Q4: Any tightening of the regulation of P2P calls would affect adversely the employment and livelihood of tens of thousands of people engaged in the telemarketing industry?

A4: The cost of maintaining the status quo is the inconvenience and nuisance caused to the majority of the population. This contrasts with the position in Singapore where a do-not-call register (for P2P calls, text messages and fax messages) was set up in early 2014 and, in an effort to enrich the value of the jobs in the domestic economy, they do not mind a reduction in the low value-add telemarketing activities. If Hong Kong follows suit, the worry about loss in jobs could be addressed by allowing a suitably long period for the transition. The proposed register could even be implemented on a sector by sector basis rather than on a full-scale basis. Assistance could be provided to the affected employees to upskill themselves to take up higher value-add jobs.

Q5: Has self-regulation by the finance, insurance, telecommunications and call centres been successful in minimising the nuisance caused to the public?

A5: It is not mandatory for telemarketers to join the trade associations of these sectors. Compliance with the relevant codes of practice drawn up by these associations is voluntary.

Q6: The proposed register would be ineffective to curb calls made outside Hong Kong, particularly if the calls are made without the use of personal data.

A6: The setting up of an accreditation system by the local telemarketing industry to raise the professional standards of its members is worth considering. Accredited callers could distinguish themselves from non-accredited callers (including those operating from outside Hong Kong) by using telephone lines bearing unique and readily-recognised prefixes (to be specially assigned by the Government).

Q7: Are the new provisions under the Ordinance good enough to deter unwanted P2P calls?

A7: The Ordinance is engaged only when the calls involve the use of personal data. The 2014 survey revealed that only 27% respondents reported that over half of the calls they received specified their names, implying that the problem of P2P calls is due more to cold calls not involving the use of personal data. The advantage of the proposed register is that it can cover all calls, including randomly generated calls without the use of personal data. Further, under the Ordinance, the consent to receive marketing messages and the subsequent exercise of opting-out are arranged on a company by company basis. By contrast, the proposed register is a one-stop-shop that enables the consumer to opt out of all unwanted telemarketing calls at one go and at the outset. Regulation under the Ordinance and setting up of the proposed register can complement each other.

A8: Is it easier for the proposed register to be set up under the Unsolicited Electronic Messages Ordinance ("UEMO") and administered by the OFCA, or under the Ordinance and administered by the PCPD?

Q8: The UEMO option should be easier. The UEMO is so structured that if it is decided in future to bring P2P calls into its ambit, such decision could be effected expeditiously by way of an amendment notice published in the Gazette under section 7. Besides, as OFCA is already administering a do-not-call register for SMS, pre-recorded messages and fax messages, it would be administratively expedient for them to take on P2P calls. The administering of the P2P call register by PDPO would not be conducive to the efficient use of public funds and the public would certainly find the arrangement confusing and less than customer-friendly.

1. 基數為曾收到人對人直銷電話的受訪者，並不包括那些從不認為直銷電話構成不便的受訪者。

All respondents who had received P2P calls, excluding those who never considered that P2P calls caused inconvenience to them.

銀行業界的資料保障
Data Protection in the Banking Industry

為了協助銀行業界在收集、儲存和使用客戶的個人資料及處理客戶的查閱資料要求時，依從條例的相關規定， 公署特別發出了一份新指引－《銀行業界妥善處理客戶個人資料指引》（「指引」）。

公署處理的投訴個案中，銀行業一直是首三大私營機構類別的被投訴者之一。此外，涉及銀行運作的投訴數字不斷增加。在 2013-14 年度，共有 373 宗此類個案，而在 2012-13 年度及 2011-12 年度則分別有 198 及 212 宗。 由於銀行業擁有龐大及敏感的客戶財務資料，發出這份指引可適切地促進及加強銀行業在處理客戶的個人資料方面依從條例的相關規定。保障私隱的銀行可以得到客戶加倍信任和支持，從而締造客戶、銀行業務及整個銀行業的三贏局面。

公署制訂這份指引時，參考了行政上訴委員會在有關案件作出的裁決、公署以往處理投訴個案的決定，以及香港銀行公會的個人資料（私隱）條例工作小組提出的意見。這份指引應對銀行業界有幫助，因為它涵蓋銀行從業員在實際工作中經常遇到的資料保障議題：

- 擬備《收集個人資料聲明》；
- 收集客戶的身份證號碼及身份證副本；
- 確保準確的客戶紀錄；
- 保留客戶的個人資料；
- 收集及使用客戶的個人資料作直接促銷；
- 與集團內其他公司共用客戶的個人資料；
- 轉移客戶的個人資料至香港以外地方；
- 披露客戶的個人資料予執法機構及財經規管者；
- 在追收欠款中使用客戶的個人資料；
- 在外展促銷活動中保障客戶的個人資料；
- 在電子銀行環境中收集及保障客戶的個人資料；及
- 處理客戶的查閱資料要求。

公署相應更新了銀行 / 金融服務的資料保障專業研習班的內容，闡釋指引的要點，歡迎業界人士參加。

The PCPD published a new Guidance Note, *Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry* ("the Guidance Note"), to assist the banking industry in complying with the relevant requirements under the Ordinance when collecting, storing and using their customers' personal data, and handling their customers' data-access requests.

Among private sector organisations, the banking industry has long been one of the top three targets of complaints. Furthermore, the number of complaints in relation to banking practices has been growing, with a total of 373 cases in 2013-14 against 198 cases in 2012-13 and 212 cases in 2011-12. Taking into consideration the large customer database maintained by the banking industry and the sensitive nature of the personal financial information involved, the PCPD considered it appropriate to publish the Guidance Note to promote and reinforce the banking industry's compliance with the Ordinance when handling their customers' personal data. Privacy-assuring banks will enjoy enhanced customer trust and loyalty, thus creating a win-win-win situation for the banks, their customers and the banking industry as a whole

The Guidance Note was compiled using references from the decisions of the Administrative Appeals Board for relevant cases, determinations in past complaint cases handled by the PCPD, and suggestions collected during meetings with the Personal Data (Privacy) Ordinance Working Group of the Hong Kong Association of Banks. The banking industry should find the Guidance Note useful as it covers real work situations commonly encountered by banking practitioners involving the following data-protection compliance issues:-

- preparing personal information collection statements;
- collecting Hong Kong Identity Card numbers and copies from customers;
- maintaining accurate customer records;
- retaining customers' personal data;
- collecting and using customers' personal data in direct marketing;
- sharing customers' personal data within the same banking group;
- transferring customers' personal data outside Hong Kong;
- disclosing customers' personal data to law enforcement agencies and financial regulators;
- using customers' personal data in debt collection;
- protecting customers' personal data in off-site marketing campaigns;
- collecting and protecting customers' personal data in the e-banking environment; and
- handling customers' data-access requests.

The content of the PCPD's professional workshops on Data Protection in Banking/Financial Services has been updated to take account of the Guidance Note. Banking practitioners are welcome to enrol in the workshops.

認識更多
Learn More

指引資料：《銀行業界妥善處理客戶個人資料》 www.pcpd.org.hk/tc_chi/resources_centre/industry_specific/files/GN_banking_c.pdf
Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry
www.pcpd.org.hk/english/resources_centre/industry_specific/files/GN_banking_c.pdf

專業研習班 www.pcpd.org.hk/tc_chi/education_training/organisations/workshops/workshop.html
Professional Compliance Workshop
www.pcpd.org.hk/english/education_training/organisations/workshops/workshop.html

強積金計劃成員投訴強積金中介人在Whatsapp披露其個人資料
Complaint about the disclosure of an MPF Scheme member's personal data on WhatsApp by an MPF intermediary

投訴人早前登記成為一間金融服務公司的強積金計劃成員，並提供她的英文姓名、流動電話號碼、住址及身份證號碼等個人資料。其後，該強積金中介人[1]自行將投訴人的資料加入其手機應用程式Whatsapp 的一個群組中，因而披露了投訴人的英文別名、流動電話號碼及個人檔案相片給該群組的其他組員。投訴人遂向私隱專員作出投訴。

結果： 投訴得直

在私隱專員進行調查的過程中，該公司確認他們就該次登記時收集了投訴人的英文姓名及流動電話號碼，不過就表示沒有收集她的英文別名，並指該別名是投訴人於 Whatsapp 自行設定的用戶名稱。該公司又解釋，該強積金中介人將投訴人加入該群組的目的是為了向她提供最新的強積金相關資訊。

由於該強積金中介人擅自將投訴人的資料加入該群組，以致投訴人的名字及流動電話號碼被第三者知悉，私隱專員認為有關做法違反保障資料第 3 原則的規定。

就是次事件，該公司已即時向該強積金中介人作出警告，提醒她要小心處理客戶的個人資料。該強積金中介人亦確認已從她的流動電話刪除該群組和投訴人的聯絡資料紀錄。

此外，該公司向其強積金中介人發出通告作出提醒，及在強積金中介人簡報會中重申，前線職員必須先取得客戶的同意方可在流動電話資訊平台及群組發佈強積金宣傳資訊，並要小心處理客戶資料，以避免不慎地將客戶資料披露給第三者。

When the Complainant registered as an MPF Scheme member with a financial institution, she provided her personal data, such as English name, mobile phone number, residential address and identity card number. The MPF intermediary[1] later added the Complainant to a group in WhatsApp, a mobile application in her mobile phone. The Complainant's English nickname, mobile phone number and photo of her profile were then disclosed to others in the group. The Complainant therefore lodged a complaint with the Commissioner.

Result: Complaint Upheld

In the course of the investigation by the Commissioner, the institution admitted that it had collected the Complainant's English name and mobile phone number at the time of the registration, but not her English nickname, which it said was the WhatsApp username set by the Complainant. The institution explained that the MPF intermediary had added the Complainant to that group for the purpose of providing her with updated MPF information.

As the MPF intermediary added the Complainant to the group without authorisation, causing disclosure of the Complainant's name and mobile phone number to third parties, the Commissioner considered that the MPF intermediary contravened Data Protection Principle 3.

With respect to this incident, the institution gave warning to the MPF intermediary reminding her to handle her clients' personal data with greater care. The MPF intermediary confirmed that the contact details of the Complainant and the group had been deleted from her mobile phone.

Moreover, the financial institution subsequently reminded its MPF intermediaries by notice and a briefing that frontline staff must obtain their clients' consent before distributing MPF promotional information in mobile information platforms and groups, and should be careful in handling client data to avoid inadvertent disclosure of the data to other parties.

1. 任職上述金融服務公司，為投訴人服務的職員。
A staff member of the financial institution who was assigned to serve the complainant.

招聘媒體承諾協助打擊匿名招聘廣告
Recruitment Media Pledge to Join the Fight against Blind Recruitment Advertisements

過去五年公署共接獲 550 宗有關匿名廣告[1]的查詢。雖然公署曾向刊登匿名廣告的機構進行循規審查及發出勸喻信，但違規行為仍然沒有減少。公署於 2014 年 3 月 15 至 22 日期間審視七個主要的廣告平台，隨機抽樣選出 71 則匿名廣告作為調查對象。公署在 2014 年 5 月 29 日公佈的調查結果顯示，當中 69 個案都是以不公平方式收集求職者的個人資料，因而違反條例保障資料第 1(2) 原則的規定。

有涉事的機構回應不知道法律規定，部分埋怨招聘媒體沒有告知或提醒其匿名廣告有不當之處，亦有刊登廣告者辯稱可以從其用作回覆的電郵地址內的公司名稱縮寫或公司全名識別公司身份，或匿名廣告沒有明確要求求職者提供其個人資料。

私隱專員並不接納上述辯解，機構不知道法律規定或埋怨招聘媒體，是不能免除其遵從條例的責任；而電郵地址並沒有提供足夠及明確的資料，以識別刊登廣告者。此外，廣告雖然沒有明示要求求職者提供個人資料，但由於僱主與求職者議價能力並不均等，一般求職者會為求得到工作，而被匿名廣告誘使提供詳細履歷。

私隱專員已向涉事的刊登廣告者發出執行通知，指令機構刪除已收集的個人資料，除非是必須為符合其他法律規定而保留資料，或為了繼續進行招聘程序；在這情況下，求職者須獲告知其資料會被保留，而他們亦有權要求刪除其個人資料。

匿名廣告顯示公司對法律的無知及不重視保障私隱及個人資料，僱主應避免刊登匿名廣告收集求職者的個人資料。如僱主確實有需要隱藏身份，可以在刊登職位空缺時使用匿名廣告，但應只限用來接受求職者的查詢，而不是收集個人資料。

招聘媒體是處於把關的最佳位置，私隱專員促請招聘媒體考慮加強識別刊登廣告者的措施，篩選接到的廣告，以識別收集求職者個人資料的匿名廣告，把不符規定的廣告退回，要求刊登廣告者作出修正，及考慮拒絕接受收集求職者個人資料的匿名廣告。

六個主要招聘媒體其後響應私隱專員的呼籲，包括求職廣場（JobMarket），Recruit，招職（JiuJik），Classified Post，JobsDB 及 Career Times。這些招聘媒體承諾會做好把關工作，防止有人透過匿名廣告不公平收集個人資料。只有 Jobfinder 未向私隱專員的呼籲作出回應。

調查報告：www.pcpd.org.hk/tc_chi/enforcement/commissioners_findings/investigation_reports/files/R14_6242_c.pdf

The PCPD has received 550 enquiries in relation to Blind Advertisements[1]. ("Blind Ads") over the past five years. Compliance checks were conducted and advisory letters were issued to the organisations placing Blind Ads, but the malpractice has continued unabated. The PCPD conducted a survey from 15 to 22 March 2014 in respect of seven major advertising platforms, and selected 71 Blind Ads on a random basis for investigation. At a press conference held on 29 May 2014, the results revealed that 69 of them were found to be in breach of Data Protection Principle 1(2) of the Ordinance for soliciting job applicants' personal data in an unfair manner.

Some of the organisations involved explained that they were ignorant of the legal requirements, while other blamed the recruitment media for not advising them or reminding them of the impropriety of their Blind Ads. Seven argued either that the company's identity could be discerned from the initials or full company name incorporated in the return email address, or that the Blind Ads did not include an express solicitation for the job applicant's personal data.

The Commissioner did not accept any of the above-mentioned defence arguments. Ignorance of the law or blaming the recruitment media did not exonerate the organisations from their obligations under the Ordinance. Email addresses did not provide sufficient, unambiguous information to identify the advertisers. Also, taking into account the disparity in bargaining power between employers and job seekers, the Blind Ads, as presented, would be more than likely to lure ordinary job seekers to provide their full curriculum vitae in an attempt to secure a job, even if there were no express solicitation of personal data in the advertisements.

The advertisers involved were issued an enforcement notice by the Commissioner directing them to delete the personal data they had collected, unless it had to be retained to satisfy certain legal requirements, or for a continuing recruitment process, in which case the job applicants had to be informed and given the option to demand the deletion of their personal data.

A Blind Ad is counter-productive as it


CTgoodjobs 向匿名廣告說「不」

Career Times 向匿名廣告說「不」。
Career Times says "No" to Blind Ads.

demonstrates the company's ignorance of the law, and disrespect for privacy and data protection. Employers should therefore refrain from placing Blind Ads seeking job applicants' personal data. Where there is a genuine need for employers to conceal their identity when advertising for job vacancies, they may resort to Blind Ads but should use them to solicit job applicant enquiries rather than personal data.

The Commissioner pointed out that the recruitment media were in the best position to act as a gatekeeper. He therefore urged them to consider stepping up their efforts to identify advertisers, screen advertisements they received to identify Blind Ads which solicited job applicants' personal data, return non-compliant ads to the advertiser for rectification, and consider refusing Blind Ads soliciting job applicants' personal data.

In response, *JobMarket, Recruit, JiuJik, Classified Post, JobsDB* and **Career Times** pledged to fight Blind Ads, heeding the Commissioner's advice to act as gatekeepers to prevent the unfair collection of personal data through Blind Ads. Jobfinder is the only recruitment media which has not responded to the Commissioner's appeal.

Investigation Report: www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R14_6242_e.pdf

1. 匿名廣告泛指機構沒有披露其身份而刊登的招聘廣告
"Blind Ads" refer to job advertisements organisations place without disclosing their identities.

補習導師及外傭中介網站過度收集及披露個人資料
Excessive Online Collection and Disclosure of Personal Data by Recruitment Agencies for Private Tutors and Foreign Domestic Helpers

公署於 2014 年 11 月 20 日公佈兩份調查報告，其中一份指六個補習中介網站在導師登記過程中收集其身份證號碼及聯絡人資料屬超乎適度，因而違反了條例保障資料第 1(1) 原則的規定，影響五十二萬名人士；另一份調查報告披露香港十家主要的外籍家庭傭工（「外傭」）中介公司，把外傭申請人的某些個人資料、其家屬及其前僱主（包括香港僱主）的個人資料上載網站任人查閱，違反了保障資料第 3 原則的規定。

補習中介網站

是次調查涉及分別由五間公司經營的六個網站。求職導師在登記時需要提供其身份證號碼及其聯絡人的姓名、電話號碼及與求職導師的關係，公署認為該些網站收集了超乎適度的個人資料。

該些網站解釋有需要收集身份證號碼以核實求職者的身份，避免出現「冒認」的情況，以防止發生影響網站及/ 或學生和家長的不正當或欺詐行為。事實上，該些網站並不是受《僱傭條例》監管的職業介紹所，沒有法律責任收集求職者的身份證號碼。它們的商業模式是低成本運作，所以並不可能面見每一位求職者以查實身份。在網上收集求職者的身份證號碼來辨識身份，可以說是毫無作用。

至於收集求職者的聯絡人姓名與電話號碼，該些補習中介網站解釋以便發生事故時可作緊急聯絡用途。這做法看來無可厚非，但該些網站應讓個別導師按其所需，自行決定是否提供聯絡人資料，而毋須在導師登記過程中強制收集。

外籍家庭傭工中介公司

另一調查報告涉及香港十間主要的持牌外傭中介公司，主要業務是為準僱主介紹有意來港工作的外傭。本案發現最大

的問題是該些中介公司在其網站展示申請人、其家屬及其前僱主（包括香港僱主）的個人資料。

外傭的工作性質有別於其他工種，她們需要長時間與僱主及其家庭成員共同生活，朝夕相對的程度猶如家人般關係密切。因此，私隱專員接納該些中介公司為協助準僱主挑選合適家傭，而在網上披露大部分申請人提供的個人資料（包括其相片）。然而，私隱專員不認同中介公司在網上披露申請人的姓名、住址、護照號碼或香港身份證號碼，他認為這些資料無助準僱主挑選合適外傭。

基於同一原因，在網上披露申請人家屬的個人資料（例如姓名、年齡及職業）及其前僱主的姓名及住址也是不被接納的。

私隱專員表示：「中介公司應該對申請人提供的個人資料逐一慎重考慮，絕不可以在網上披露與申請人求職目的並無直接關係的個人資料。這做法與直接向親身到中介公司的準僱主披露個人資料截然不同，分別是申請人提供的個人資料一旦在網上公開，便可能被不知名的第三者隨意查閱、複製甚至永久保存，及與其他零碎但屬同一人的個人資料整合。任何人也難以預料及控制誰人可以再次使用有關資料。」

改善措施及執法行動

私隱專員欣悉部分外傭中介公司已在調查期間採取了相關的改善措施。為確保有關機構完全遵守條例規定，私隱專員已向該十家外傭中介公司及五間經營補習中介網站的公司分別送達執行通知，指令他們要採取措施糾正尚有違例的情況，例如採用編號以代替在網上指示申請人姓名等，以及防止違例的情況再次發生。

機構及消費者都必須了解，進行電子商貿活動及使用網上服務平台可能帶來私隱風險，例如資料外洩、資料被不明人士再使用，從而對當事人造成不必要的滋擾及身份盜竊。經營網站的機構須確保它們收集及使用的個人資料真正符合業務所需，而消費者習以為常地在網上向服務供應商提供個人資料亦應多加警惕，不要因為急於獲取某些服務而白白犧牲自己的個人資料私隱。

私隱專員補充：「作為良好的行事方式（而非只為遵守條例規定），即使申請人的有關個人資料客觀地有助準僱主挑選合適家傭，我建議外傭中介公司在網上披露該些資料前，最好先取得申請人的同意。鑑於網上披露資料所帶來的私隱風險，及部分資料屬敏感性質，這良好的行事方式是更妥善的做法。外傭中介公司須尊重申請人的選擇，不應上載申請人表示不同意在網上披露的個人資料。」

公署將聯同有關商會於 2014 年 12 月至 2015 年 1 月期間舉行三場講座，協助外傭中介公司了解條例的規定。

調查報告全文：
（補習中介網站）www.pcpd.org.hk/tc_chi/enforcement/commissioners_findings/investigation_reports/files/R14_19675_c.pdf
（外籍家庭傭工中介公司）www.pcpd.org.hk/tc_chi/enforcement/commissioners_findings/investigation_reports/files/R14_1382_c.pdf

The PCPD published two investigation reports on 20 November 2014. One report revealed six tutorial service agency websites in breach of Data Protection Principle ("DPP") 1(1) of the Ordinance for unnecessarily collecting the Hong Kong Identity Card ("HKID Card") numbers of private tutors and the personal particulars of their contact persons during online registration. About 520,000 persons were affected. The other investigation report revealed 10 major employment agencies for domestic helpers in breach of DPP3 for posting on their websites the personal data of overseas job applicants, members of their families and their past employers (including Hong Kong employers).

Tutorial Service Agency Websites

The investigation covered five website operators and six websites. Job seekers who wished to be enrolled in the placement service must provide their HKID Card number and a contact person with name, telephone number and relationship with the job seeker. This amounted to excessive collection of personal data by the websites.

The websites argued that collection of the HKID Card numbers was necessary to authenticate the identity of the job seekers to prevent impersonation and other improper or fraudulent activities which could be committed by job seekers to the detriment of the websites and/or the parents and students. In fact, the website operators are not employment agencies regulated under the Employment Ordinance, so they have no legal obligation to collect job seekers' HKID Card numbers. Operating on a low-cost model, they do not interview job seekers in person for employment checking and identity verification, so collecting job seekers' HKID Card numbers online for identification is a farce.

The website operators also explained that they require the name and telephone number of the job seeker's contact person as a fall-back or emergency contact in the event the job seeker cannot be reached or gets into trouble. While these explanations may make sense on some occasions for some job seekers, job seekers must be given the option of not providing a contact person with name and telephone number. The mandatory provision of the data should not be made a prerequisite for service enrolment.

Employment Agencies for Foreign Domestic Helpers

The investigation covered 10 major employment agencies for foreign domestic helpers registered under the Employment Ordinance. Their business is to recruit job seekers from overseas for placement as domestic helpers with employers in Hong Kong. The major problems revealed in the investigation were posting on the agencies' respective websites the personal data provided by the job seekers, which related to the job seekers themselves, their family members and their past employers, including Hong Kong employers.

Domestic helpers perform their jobs in unique circumstances, in that they live with the family of their employer and are often treated as a member of

the family, interacting intimately with all family members day in and day out. The Commissioner therefore accepts the agencies' posting on their websites most of the personal data provided by the job applicants, including their photos, as they help prospective employers screen helpers. However, the posting of the job applicants' names, addresses, and passport and/or HKID Card numbers is not acceptable because it is inconceivable that this data serves an instrumental role in the prospective employer's initial selection process.

For the same reason, the display on their websites of the personal data (e.g. name, age and occupation) of the job applicants' family members and past employers' names and addresses is not acceptable.

The Commissioner commented, "Unlike presenting the job seeker's profile to the prospective employer in person when the latter visits the agencies' offices, displaying her personal data online allows unrestricted access by unidentified third parties, who may copy the data, retain the data permanently, and integrate or correlate the data with other fragmented data about the same person from different sources. The possible secondary use of such data is beyond the average person's anticipation or comprehension, and definitely very difficult to control."

Remedial Actions and Enforcement Action

During the course of the investigation, the Commissioner was pleased to note that certain remedial action had been taken by some of the employment agencies for foreign domestic helpers. To secure full compliance with the Ordinance, the Commissioner served enforcement notices to the 10 employment agencies and the five tutorial service website operators, directing them to take steps to remedy the contraventions for which remedial actions were outstanding, for example, replacing the names of the job applicants on the Internet by reference numbers, and prevent the recurrence of all known contraventions.

Organisations and consumers who engage in e-commerce and other online services must be aware of the associated privacy risks, such as data breaches and unanticipated secondary use of the data by unknown third parties, including unwanted communication and identity theft. Website operators must ensure that they are capturing and using personal data for reasonable business purposes. Web consumers accustomed to submitting personal information to various service providers in order to obtain desired services must be more vigilant about providing such information.

"I would further advise that as a matter of best practice (not just compliance with the provisions of the Ordinance), employment agencies should first obtain the consent of job applicants for the online display of their personal data even though objectively the data is relevant to employee selection by prospective employers. Going this extra mile is recommended in view of the privacy risks associated with posting information online and the sensitivity of some of the information posted. Employment agencies should respect the choice made by the job applicants and refrain from uploading information an applicant does not want online," the Commissioner remarked.

In conjunction with the trade associations, three educational seminars will be held by the PCPD in December 2014 and January 2015 for all operators of the employment agencies for foreign domestic helpers.

Full Investigation Reports:
(The Tutorial Service Agency Websites) www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R14_19675_e.pdf

(The Employment Agencies for Foreign Domestic Helpers) www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R14_1382_e.pdf

視察報告建議勞工處就業服務優化個人資料系統
Inspection Report Conducted to Assist the Labour Department's Employment Service Improve its Personal Data System

公署根據條例第 36 條，在 2014 年 3 月至 7 月期間視察勞工處就業服務的個人資料系統，並於 11 月 20 日發表報告。鑒於很多其他政府部門及公營機構提供公共服務，都會採用類近勞工處的方式來收集及處理個人資料，私隱專員建議這些部門及機構可以本報告作為借鏡。

視察報告：www.pcpd.org.hk/tc_chi/enforcement/commissioners_findings/inspection_reports/files/R14_3849_c.pdf

From March to July 2014, the PCPD inspected the personal data system of the employment service of the Labour Department ("LD"), pursuant to section 36 of the Ordinance, and released a report on 20 November 2014. The Commissioner pointed out that the LD's method of collecting and processing the personal data of members of the public for delivering public services was typical of many government departments and public organisations, who are encouraged to take reference from this report to ensure compliance with the requirements under the Ordinance.

The Inspection Report: www.pcpd.org.hk/english/enforcement/commissioners_findings/inspection_reports/files/R14_3849_e.pdf

私隱專員就《電子健康紀錄互通系統條例草案》提交意見書
The Commissioner Raises Concerns on the Electronic Health Record Sharing System Bill

毫無疑問這個電子健康紀錄互通系統(在立法會法案委員會討論中)可以讓獲授權的醫護人員取得及互通參與病人的病歷，令到以病人為本的醫護協作模式更有效率，但亦同時對保障私隱及個人資料方面構成重大挑戰。鑑於健康資料性質非常敏感及私人，私隱專員認為新法例在病人病歷方面提供的私隱保障，不能低過現行《個人資料(私隱)條例》所提供的保障。

私隱專員並於2014年5月21日向立法會《電子健康紀錄互通系統條例草案》委員會及其後法案委員會會議中，提交了就相關草案的意見書，提出了多項有關個人資料私隱保障方面的關注包括：

1. 新法例的條文應該向公眾清楚闡述，這個互通系統會設計成可把病人病歷的健康資料分門別類，令醫護專業人員嚴格按「有需要知道」的情況，才可查閱病人相關的健康資料。
2. 互通系統應該提供一個「保險箱」，以儲存病人的某些特別敏感的病歷資料，及加強控制查閱該些資料。若有這項功能，病人便可以令個別醫護提供者，即使已取得病人的一般同意，也不可自動取覽部分類別的健康紀錄互通資料。
3. 電子健康紀錄專員可允許「直接或間接提供醫護服務」的團體和「涉及提供醫護服務」的政策局或部門在互通系統登記，該酌情權似乎過於寬鬆。
4. 即使是「獲書面授權的人士」也不能代表資料當事人對其儲存於互通系統的健康資料行使查閱及改正權利，這安排看來並不合理。
5. 草案建議對於未獲授權經電腦查閱互通系統內的健康資料訂為罪行；公署建議應考慮把未獲授權下採用其他途徑查閱電子健康紀錄的行為或不當使用該些資料，也同樣訂為罪行。
6. 根據草案，電子健康紀錄專員並無法律責任檢視已登記的醫護提供者的電子醫療紀錄系統。公署認為，這實際上會削弱及貶低電子健康紀錄專員規管及監管互通系統中共享及使用健康資料，以及監管參與的醫護服務提供者遵守新法例的法定職能。

意見書的全文已刊於 www.pcpd.org.hk/tc_chi/news_events/speech/files/eHR_summary_legco_paper_c.pdf。

There is little doubt that the Electronic Health Record System (being discussed by the Bills Committee of the Legislative Council), designed for access to, and sharing of, participating patients' health data by authorised healthcare providers, can provide collaborative patient-centred care more efficiently. But it also poses serious challenges to privacy and data protection. In view of the very sensitive and private nature of health data, the Commissioner recommended that the new legislation under discussion provide privacy safeguards to patients' health data at a level no less than that provided under the existing Personal Data (Privacy) Ordinance.

The Commissioner expressed his concern about the Electronic Health Record Sharing System (the "System") Bill in his submission (the "Submission") to the Bills Committee on 21 May and at these subsequent Bills Committee meetings. The major concerns raised in the Submission are as follows:-

1. It should be made clear that compartmentalisation of data will be introduced as a basic design feature of the System so that healthcare professionals can access the health records of a patient only on a strictly "need-to-know" basis.
2. The System should provide a "safe deposit box", which allows the separate storage of certain particularly sensitive patient data, with enhanced access control, thus allowing patients to prevent some categories of sharable data from being automatically viewable by healthcare providers even with prior generable consent obtained from the patients.
3. The discretion of the Electronic Health Record Commissioner to allow registration under the System of bodies who "directly or indirectly provide healthcare" and government bureaus or departments involved in "providing healthcare" seems too wide.
4. Denying patients the right to authorise a representative in writing to exercise their data access and correction rights in respect of their health data kept in the System seems unreasonable.
5. In line with the provision in the Bill to create a specific offence for unauthorised access to the health data held in the System through the use of computers, consideration should be given to introducing offences for unauthorised access of such data by any other means and for unauthorised use of the data.
6. Relieving the Electronic Health Record Commissioner of the legal obligation to inspect the information systems used by the healthcare providers participating in the System in effect belittles and discredits the Commissioner's statutory functions to regulate and supervise the sharing and use of the health data kept in the System, and to supervise the participating healthcare providers' compliance with the new legislation.

Full details of the submission are at www.pcpd.org.hk/english/news_events/speech/files/eHR_summary_legco_paper_e.pdf.

與Facebook就個人資料保障會面
Dialogue with Facebook on Personal Data Protection

Facebook副首席私隱主任Rob Sherman（左一）與一眾私隱倡議者交流能界。

Deputy Chief Privacy Officer Mr Rob Sherman (first from left) of Facebook exchanges views with the PCPD and other privacy advocates.

美國Facebook公司副首席私隱主任Rob Sherman應公署的邀請來港出席2014年5月的「關注私隱運動」，向公署、私隱倡議者、企業及學生講述Facebook保障私隱的政策框架和新措施。公署與Facebook會面間，公署要求Facebook向香港Facebook用戶公開承諾他們同樣享有Facebook向美國及歐盟民眾提供的資料保障措施，包括因應愛爾蘭資料保障專員對其所進行的審查及美國聯邦貿易委員會的和解協議而新增的措施，例如在改變用戶的私隱設定之前，要取得他們的明確同意；30日內妥善執行刪除資料要求；以及不會作出有關私隱保障方面的失實陳述。

公署強調Facebook應透過其私隱政策、私隱警告、私隱設定和其他工具，提供清晰、具透明度及易於使用的方式，讓用家可以掌控自己的個人資料。公署亦要求Facebook香港用戶提供教育活動，使他們了解如何使用各項設定以有效地保障自己的個人資料，及遇上網絡欺凌及網絡罵戰時，該如何處理。

During Privacy Awareness Week ("PAW") in May 2014, Deputy Chief Privacy Officer Mr Rob SHERMAN of Facebook Inc. ("Facebook") flew in from the U.S. by invitation of the PCPD to address concerns and exchange views with the PCPD, privacy advocates, business people and students on Facebook's privacy protection policy framework and new measures implemented in the US and EU. In Mr Sherman's exchange with PCPD senior executives, the PCPD invited him to openly commit to Hong Kong Facebook users that they would be accorded the same privacy protection safeguards that applied to US and EU residents. These safeguards include measures introduced as a result of the Irish Data Protection Commissioner's audits and the US FTC settlement (such as obtaining express consent from users before overriding their privacy settings, to honour deletion requests within 30 days, and not to make misrepresentations about their privacy protection).

The PCPD stressed that Facebook should provide clear, transparent and accessible means by way of their privacy policies, privacy warnings, privacy settings and other tools to empower individuals to control their own personal data. Facebook was also requested to establish an education programme for Hong Kong users to reach out to them to explain how their Facebook settings could be used effectively to protect their personal data privacy, and what to do in case they fell victim to cyber bullying or cyber flaming on Facebook.

私隱及資料保障法律獎學金
Scholarship for the Study of Privacy and Data Protection Law

香港大學法律系學生毛茅獲頒私隱及資料保障法律獎學金。

HKU LLB Student Adela Mao is awarded the Privacy Commissioner Prize in Privacy and Data Protection Law.

公署由2012年起與香港大學法律學院合辦獎學金，鼓勵法律系學生關注個人資料私隱這個課題。今年，香港大學法律系五年級學生毛茅以「私隱保障於網絡時代的挑戰」為題的論文，從七份作品中脫穎而出獲獎。

The PCPD and the Faculty of Law of The University of Hong Kong ("HKU") jointly set up a scholarship called "Privacy Commissioner Prize in Privacy and Data Protection Law" in 2012 to encourage law students to study data-privacy issues. This year, seven entries were received. Adela MAO, a HKU LLB Year 5 student, won the Prize with her research paper The Legitimizing Ground of "Consent" in the Personal Data Protection Regime in Hong Kong.

關注私隱運動 2014 - 個人資料私隱：自己作主話事
Privacy Awareness Week 2014 - Personal Data Privacy: Have My Say

一年一度的「關注私隱運動」於 5 月 4 日至 10 日期舉行，期間公署推出了一連串公眾教育活動，號召市民及企業坐言起行，保護個人資料私隱。「關注私隱運動」是亞太區私隱機構（Asia Pacific Privacy Authorities）成員合作的年度推廣項目。今年參與的地區包括澳洲、加拿大、哥倫比亞、澳門、墨西哥、新西蘭、南韓、秘魯及美國。

在該星期超過 500 名保障資料主任聯會的會員亦各自在其公私營機構內舉行提高私隱意識的推廣活動。

公署一直致力走進社區，特別是年青人的範疇。保障私隱學生大使在「關注私隱運動」的一星期在各中學展開多樣化的推廣宣傳活動。

為期一星期的「關注私隱運動」共有超過 5,200 名中學生及 5,400 名公眾人士參與，比去年同一活動增加了 173 %。

詳情請瀏覽「關注私隱運動」網站：
www.pcpd.org.hk/paw

In Privacy Awareness Week ("PAW") 2014, from 4 to 10 May, the PCPD rolled out a series of public education activities, calling upon the public and businesses to protect personal data privacy. PAW is an annual promotion event jointly held by members of the Asia Pacific Privacy Authorities ("APPA"). This year, the event was celebrated in Australia, Canada, Colombia, Macao, Mexico, New Zealand, South Korea, Peru and the United States.

During the week, over 500 members of the Data Protection Officers' Club ("DPOC") initiated their own privacy awareness programmes in their respective organisations.

The PCPD's goal was to actively engage the community, in particular, young people. During PAW, Student Ambassadors for the PCPD's Privacy Protection Programme organised campus promotion exercises in their schools.

私隱專員蔣任宏與教育局局長吳克儉帶領保障私隱學生大使，為「關注私隱運動 2014」揭開序幕。

Mr Allan Chiang, Privacy Commissioner for Personal Data, and Mr Eddie Ng, Secretary for Education, lead student ambassadors in the launch of PAW 2014.

公署在該星期出版了《機構智用社交網絡 尊重個人資料私隱》資料單張。同時在香港互動市務商會的支持下，舉行了「機構使用社交網絡：私隱保障的重要」講座吸引了超過 180 名人士出席。香港科技大學商學院資訊、商業統計及營運學系教授許佳龍教授（左二）、Facebook 副首席私隱主任 Rob Sherman（右二）、CMRS Digital Solutions Ltd. 創辦人司徒廣釗先生（右一）擔任講者。

During PAW, in conjunction with the release of the information leaflet "Privacy Implications for Organisational Use of Social Networks", a seminar titled "Using Social Networks by Organisations: Why Privacy Matters" has been held with the support of the Hong Kong Association of Interactive Marketing, attracting over 180 attendees. Professor Hui Kai-lung (second from left) from Department of Information & Systems Management, The Hong Kong University of Science & Technology Business School, Mr Rob Sherman (second from right), Deputy Chief Privacy Officer, Facebook and Mr Ralph Szeto (first from right), Managing Partner, CMRS Digital Solutions Ltd. have been invited to speak in the seminar.

The one-week PAW 2014 attracted the participation of over 5,200 students and about 5,400 other members of the public, an 173% increase over last year.

Visit our website for more details at www.pcpd.org.hk/paw.

教育局局長吳克儉在同一典禮上，頒發獎項予保障私隱學生大使計劃 2014 暨中學生關注私隱專題報道比賽高級組冠軍伊利沙伯中學、亞軍佛教沈香林紀念中學及季軍趙聿修紀念中學的參賽隊伍。

Secretary for Education Mr Eddie Ng presents awards to the champion from Queen Elizabeth School, the first runner-up from Buddhist Sum Heung Lam Memorial College and the second runner-up from Chiu Lut Sau Memorial Secondary School in the senior section of the News Reporting Competition under Student Ambassador for Privacy Protection Programme 2014.

公署與香港青年協會賽馬會Media 21媒體空間合辦了網上直播講座「社交網絡私隱　自己作主話事」及青少年網上私隱論壇，與中學生就網上私隱問題互相交流。香港青年協會督導主任徐小曼女士（左一）、公署資訊科技顧問張宗頤博士（左二）及Facebook 大中華區廣告代理業務總經理黃緯賢先生（右一）與中學生討論如何在網上保障私隱。

A web-cast forum "Have May Say – How to Use Social Networks While Protecting Privacy" and a Youth Forum on Online Privacy have also been organised, in collaboration with the Hong Kong Federation of the Youth Groups. Ms Hsu Siu-man (first from left), Supervisor from The Hong Kong Federation of Youth Groups, Dr Henry Chang (second from left), IT Advisor of the PCPD and Mr Andrew Wong (first from right), Head of Agency/Reseller – Greater China, Facebook discuss with students tips for protecting online privacy.

2014年學生大使計劃「中學生關注私隱專題報道」比賽的參賽學生透過其得獎作品，在校園宣揚保障人資料訊息。

The winning teams of the News Reporting Competition under the 2014 Student Ambassador for Privacy Protection Programme share the messages of personal data protection on campus.

公署藉著公共圖書館的資訊科技講座及在港鐵站舉行保障個人資料展覽，走進社區，希望更有效地向公眾傳揚個人資料私隱保障的意識。

As part of our community outreach programme, we have organised an IT seminar at a public library and an exhibition at MTR Hong Kong Station to spread the message of the importance of data privacy protection to members of the public.

「關注私隱運動」是亞太區私隱機構（Asia Pacific Privacy Authorities）成員合作的年度推廣項目。今年公署與澳門個人資料保護辦公室在上環港鐵站(港澳碼頭)聯合以海報宣傳下載應用程式安全的信息。

PAW is an annual promotion event jointly held by members of the APPA. This year the PCPD and the Office for Personal Data Protection, Macao promote safe use of mobile apps by an advertisement in MTR Sheung Wan Station (Hong Kong Macau Ferry Terminal).

第 36 屆國際資料保障及私隱專員研討會
The 36th International Conference of Data Protection and Privacy Commissioners

在 2014 年 10 月 13 至 16 日，私隱專員出席了在毛里求斯巴拉克拉瓦舉行的第 36 屆國際資料保障及私隱專員研討會，並在會上分享如何把保障私隱及資料納入企業管治責任其中。

會議通過「毛里求斯宣言－物聯網」，並就大數據、執法合作及數碼年代的私隱通過決議案，認同物聯網及大數據引起人們對個人私隱與公民權利、免受歧視的保障，及侵犯平等待遇權利這些事宜的重大關注。

The Commissioner attended the 36th International Conference for Data Protection and Privacy Commissioners in Balaclava, Mauritius from 13 to 16 October 2014, where he shared ideas on how to manage privacy and data protection as corporate governance responsibility.

The conference passed the "Mauritius Declaration on the Internet of Things" and resolutions on Big Data, Enforcement Cooperation and Privacy in the Digital Age, which acknowledged that the internet of things and big data raise "important concerns with regard to the privacy of the individuals and civil rights, protections against discriminatory outcomes, and infringements of the right to equal treatment."

一名人士向私隱專員作出虛假陳述被判監禁
A Person was Sentenced to Imprisonment for Making False Statement to the Commissioner

一名前保險代理（「該代理」）在 2014 年 11 月 20 日被控兩項違反條例第 50B(1)(c)(i) 條向私隱專員作出虛假陳述的罪名、一項違反《盜竊罪條例》第 16A 條的欺詐罪名，及五項違反《刑事罪行條例》第 73 條的使用虛假文書罪名。該代理承認控罪，被判監禁四個星期。今次是條例自 1996 年生效以來，首宗在私隱專員執行其法定職能的過程中因誤導私隱專員而違反條例規定被判有罪的個案。

個案源於一宗公署於 2012 年 10 月接獲的投訴。投訴人是一間保險公司的客戶，該代理在有關保險公司工作時曾接觸投訴人。其後，該代理轉職另一間保險公司，並游說投訴人購買一份新保單，但投訴人當時並不知道新保單的承保人是該代理轉職後的另一間公司。投訴人指稱該代理誤導她，以不公平的方法取得她的個人資料。

該代理回應公署的查詢時提供虛假資訊，干犯條例下的罪行。公署把個案轉介警方作刑事調查，進一步揭露保險的文件中部分簽名並非由投訴人簽署。

公署提醒所有機構及個人須遵守法例，嚴肅對待個人資料私隱。涉及投訴的任何人士在回應公署的查詢時，應與公署合作如實提供資料。

A former insurance agent (the "Agent") was charged with two counts of making a false statement to the Commissioner under section 50B(1)(c)(i) of the Ordinance, one count of fraud under section 16A of the Theft Ordinance and five counts of using a false instrument under section 73 of Crimes Ordinance on 20 November 2014. The Agent pleaded guilty to the charges and was sentenced to 4 weeks' imprisonment. Since the enforcement of the Ordinance in 1996, this is the first conviction for contravention of the Ordinance by misleading the Commissioner in discharging his statutory functions.

The case stemmed from a complaint from a customer of an insurance company received by the PCPD in October 2012. The Agent had approached the complainant while working for one insurance company. He subsequently moved to another insurance company and sold a new insurance policy to the complainant who was unaware, at the time, that the policy bought was issued by the latter company. The complainant alleged that the agent had misled her, and had thereby obtained her personal information by unfair means.

In responding to the PCPD's enquiries, the Agent gave false information to the PCPD, which constituted an offence under the Ordinance. The case was referred to the Police for criminal investigation which unearthed that some of the signatures on the insurance documents were not signed by the complainant at all.

The PCPD reminds all organisations and individuals to abide by the law and treat personal data privacy seriously. Parties involved in a complaint should cooperate and be truthful in responding to PCPD's enquiries.

為零售業界推出定期培訓及網上評估工具
Launch of Regular Training Programmes and Online Assessment Tool for the Retail Industry

公署與香港零售管理協會於2013年6月携手推動「零售業保障個人資料私隱活動」，目的是增進零售業界對條例的認識，並鼓勵他們採取良好的行事方式。是次活動在2014年8月閉幕，鑒於零售業前線員工在培訓方面有一定需求，再加上不少零售商視保障個人資料為顧客服務的必備元素，公署在網站提供了特別為零售業而設的網上評估工具，協助業界培訓和測試前線員工對條例的理解。此外，公署會繼續舉辦「零售業保障私隱面面觀」研習班，使之成為公署的常規培訓項目。研習班會按零售業前線人員會涉及處理個人資料的常見處境例如會藉及續會申請、抽獎活動、直接促銷、使用閉路電視、招聘員工及手機應用程式，向從業員講解如何遵從條例要求保障個人資料，並提供簡易的指引和實用貼士。

零售業網上評估工具(www.pcpd.org.hk/misc/retail/online_train.html)
Online assessment tool tailor-made for the retail industry (www.pcpd.org.hk/misc/retail/online_train.html)

The new regulatory regime for direct marketing under the Ordinance , which came into effect in 2013, has generated immense training interest from the retail industry. To address this interest, the PCPD, in partnership with the Hong Kong Retail Management Association, launched a privacy campaign, called "Driving Retail Excellence through Privacy Assurance" ("the Campaign"), in June 2013, with a view to promoting understanding of the data protection requirements under the Ordinance and encouraging the adoption of good privacy practices. The Campaign was fruitfully concluded in August 2014. To meet the demand for training frontline salespeolpe and to tie in with the recognition by the industry that personal data protection is a prerequisite for good customer service, the PCPD has made available on its website a new online assessment tool tailor-made for the retail industry. Retail practitioners are encouraged to use the assessment tool for training or evaluating the level of understanding of the Ordinance among their frontline staff.

The PCPD will also continue to organise the Workshop on Retail Operations as part of its regular training programmes. This workshop provides guidance on compliance with the Ordinance and tips for handling personal data protection in different scenarios of retail operations, such as membership renewal, lucky draws, direct marketing, the use of CCTV, staff recruitment and use of mobile apps.

大中華私隱研討會
Symposium on Privacy in Greater China

私隱專員於2014年11月28日在香港大學法律及資訊科技研究中心舉辦的大中華私隱研討會上發表專題演說，題目為「管理私隱及資料保障為企業管治責任」。

The Commissioner delivered a keynote speech on 28 November 2014 on the topic "Managing Privacy and Data Protection as Corporate Governance Responsibility" at the Symposium on Privacy in Greater China organised by Law and Technology Center, The University of Hong Kong.

榮獲 2014 年「申訴專員嘉許獎」
Winning the Ombudsman's Award

公署個人資料主任盧迪凡先生於 2014 年 10 月 30 日舉行的「2014 申訴專員嘉許獎頒獎典禮」上獲頒公職人員獎。該獎項設立的目的，是表揚在處理投訴方面達到專業水平的政府部門及公營機構，同時在公共服務範疇推動正面的服務文化。

盧迪凡先生表示：「能協助受屈者是我處理投訴時最大的樂事，也是推動我積極處理投訴的動力。」

Personal Data Officer Mr D F LO was awarded the Ombudsman's Award 2014 for Officers of Public Organisations at the 18th Ombudsman's Awards Presentation Ceremony on 30 October 2014. The Ombudsman's awards aim to acknowledge professionalism in handling complaints and to foster a positive culture of service in the public sector.

公署個人資料主任盧迪凡先生榮獲 2014 年「申訴專員嘉許獎」
Congratulations to our Personal Data Officer, Mr D F Lo, who has won the Ombudsman's Award 2014.

"Helping the aggrieved is a very pleasant experience for me when handling complaints, and it motivates me to keep up my work," said Mr Lo.

保障私隱學生大使計劃 2015 –「私隱檔案」新聞攝製比賽
Student Ambassador for Privacy Protection Programme 2015 – TV News Feature on Personal Data Protection Competition

專為中學生而設的「保障私隱學生大使計劃」已經展開，今年已是公署連續第五年舉辦這個活動。該計劃是與星島雜誌集團合辦的，並獲得教育局全力支持。活動今年舉辦一個以「私隱檔案」為題的新聞攝製比賽，邀請全港中學生透過新聞專題報道形式，探討個人資料私隱的熱門話題。有超過七百名來自 69 間不同中學的學生參加。

The PCPD launched a Student Ambassador for Privacy Protection Programme, the fifth in a series of annual programmes designed for secondary school students. It is jointly organised with Sing Tao Magazine Group and fully supported by the Education Bureau. This year, the programme features a news reporting competition. Secondary school students were invited to create TV news reports on topical issues related to personal data privacy. Over 700 students from 69 different secondary schools enrolled in the competition.

為讓參賽學生掌握個人資料保障的知識和拍攝新聞短片的技巧，公署於 11 月 8 日舉行比賽工作坊，由公署職員講解相關保障私隱要點，並特別邀請香港電台電視部紀錄片監製方曉山先生 (左二) 及新聞工作者／電視節目主持人柳俊江先生 (左一) 與學生分享新聞從業員的經驗。
To better equip the students with knowledge of personal data protection and skills for TV news production, the PCPD organised a seminar on 8 November. Mr Fong Hiu-shan (second from left), Executive Producer of RTHK's Documentary Section (TV), and Mr Ryan Lau (first from left), a journalist and a host of TV news programmes, are invited to share their journalism experience with the students.

公署網站新面貌
A Vibrant New Look for the PCPD's Website

公署網站自 1996 年 12 月啟用以來，一直是公署向公眾提供資訊的主要途徑，公眾可使用這便捷平台取得與私隱課題相關的資料。

全新面貌的公署網站於本年 11 月推出。不單更新了主頁的設計，更重新編排網站內容，及新增多項功能， 藉以提供一站式的平台，主要新功能包括：

- **回應式設計（Responsive Design）**
  因應裝置的螢幕自動調節畫面大小，為各類裝置（桌面電腦以至流動電話）提供最佳的觀感。
- **使用者為本**
  提供「捷徑」讓用家可按「個人」（即資料當事人）及「機構」（即資料使用者）的需要，較快捷地獲取相關的資訊。
- **加強搜索功能**
  提供四項搜索功能（關鍵字搜索、進階搜索、熱門搜索及個案簡述搜索）以提升搜索效率。
- **無障礙功能**
  採用符合萬維網聯盟《無障礙網頁內容指引》2.0 版 AA 級別標準的無障礙網頁設計，讓普羅大眾包括殘疾人士或受色盲困擾的人士，獲取網上資訊。
- **社交媒體分享**
  公眾可透過社交網站分享現時已上載至公署網站的資訊，擴闊公署的網上平台。
- **簡便指南**
  提供更快捷的方法瀏覽公署最受歡迎的頁面。

公署網站會在不久將來陸續推出新功能，例如在網上報名參加公署的講座及簡體中文版。

The PCPD's website was created in December 1996 and has become an important channel for the PCPD to reach out to the community. People find the website a convenient platform to obtain a growing wealth of privacy information. However, a revamp became necessary to ensure a user-friendly online presence.

The website underwent a face-lift in July and was completely redesigned in November this year, with the contents restructured and a host of new features incorporated to provide a one-stop portal on privacy-protection matters. Some of the major enhancements are listed below:

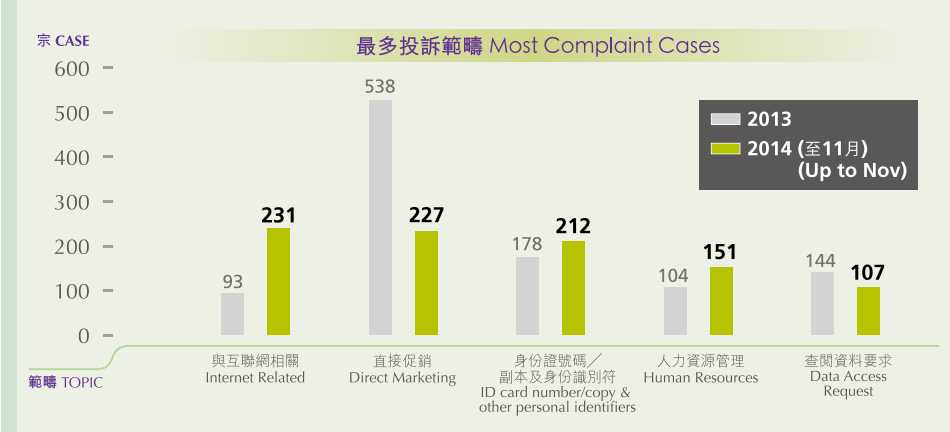
- **Responsive Design**
  Pages are automatically adjusted according to a device's screen size to provide an optimal viewing experience across a wide range of devices (from desktop computer monitors to tablets and smart phones).
- **User-oriented approach**
  The new website provides shortcuts for direct access / retrieval of information respective to "individuals" (data subjects) and "organisations" (data users) which are relevant to their needs.
- **Improved searchability of information**
  It has enhanced search functions (i.e. Keyword Search, Advanced Search, Hot Search and Case Notes Search).
- **Improved accessibility**
  The site conforms with World Wide Web Consortium Web Content Accessibility Guidelines 2.0 Level AA requirements to facilitate access by the widest possible audience, including persons with disabilities or with specific difficulties, such as colour-blindness.
- **Social Media Sharing**
  The website enables information on the PCPD website to be shared via popular social media platforms to enhance the PCPD's on-line presence.
- **Quick Guide**
  This provides quicker access to the most popular pages.

More new features will be rolled out in near future, such as online registration for PCPD's seminars and simplified Chinese version of the website.

接獲投訴個案
(2014年1月至11月)

Number of complaint cases received
(January - November 2014):

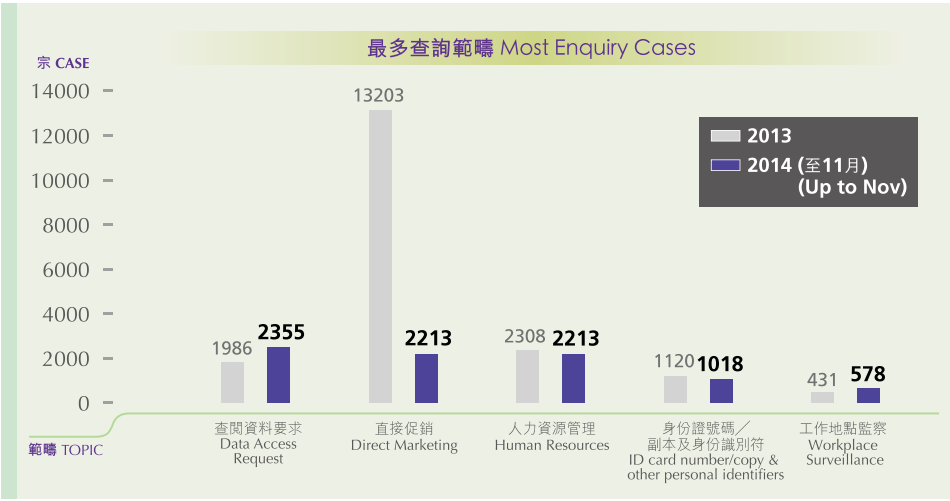
共 1,549 宗 cases



接獲查詢數目
(2014年1月至11月)

Number of enquiry cases
(January - November 2014):

共 16,083 宗 cases



無線射頻識別（RFID）帶來甚麼私隱風險？
What are the Privacy Implications of Radio Frequency Identification?

無線射頻識別（RFID）是利用無線電波傳輸資料往返閱讀器的電子標籤。RFID 晶片通常記載著資料，在有效距離範圍內的閱讀器要求讀取時，便會釋放資料，用作追蹤及識別該晶片所依附的物件。RFID 晶片用途廣泛，在零售業的使用越來越普遍，因它有助更有效地控制貨品的流程、補給及管理。

RFID 晶片一般會隱藏在產品中，不易被看見；加上這些產品往往是由人所使用或攜帶，有關產品和個人均可在全不知情的情況下被追蹤。

由於大多數 RFID 晶片有下述特性，使用 RFID 標籤會對私隱帶來某些影響：

- **持續運作**：
  RFID 標籤是不能關掉的，因為其能源通常是由閱讀器以無線電波遙距提供。當閱讀器接近時，標籤便會啟動，內裡記載的資料即可被讀取。
- **沒有明顯控制**：
  就算擁有標籤的人沒有明確「授權」，RFID 標籤都會自動回應閱讀器，所以 RFID 標籤可以在該人不知情或沒有給予同意的情況下運作及提供資料。
- **無線電通訊**：
  利用閱讀器讀取 RFID 標籤是相對容易，而且標籤與閱讀器的互動通常是看不到的。因此，別人讀寫你身上的 RFID 標籤時你也可能不會察覺到。
- **公開標準**：
  產品所使用的 RFID 標籤大部分記載有一套標準產品電子代碼，任何人可以輕易地翻查，找出標籤所依附的產品的詳情。利用 RFID 閱讀器掃瞄電子代碼後，便有機會找出某人所穿帶的物品資料（包括衣服尺碼及牌子、藥瓶、書籍類型等），從而了解某人的身體狀況、個人喜好等。

要留意的是，用作標籤物品的 RFID 晶片的操作距離是一般是一至四米，標籤內容因此可以在較遠的距離被讀取。如晶片在產品離開銷售點後仍被保留在產品內，在讀取晶片可能儲存的資料（獨特識別碼、產品資訊等）後，可能會對消費者的私隱構成以下威脅：

- **追蹤位置**：
  每個標籤都有獨特的製造識別碼。如能把這識別碼與特定的人聯繫，然後在不同地點閱讀有關標籤，便可以追蹤他的位置。例如，一個人穿著附有標籤的 T 恤，其位置便可被追蹤。
- **資料外洩**：
  只要閱讀藏在某人攜帶的物品中的標籤，例如護照、書籍、手錶及藥瓶，便可以收集有關該人的資料，輕易地推斷其個人喜好、健康狀況，甚至政見。

如無進行私隱影響評估，RFID 標籤有可能對消費者的私隱構成威脅。有關方面，尤其是零售業，應採取對策防止使用 RFID 標籤而可能引發的私隱問題：

- 設計需要在掃瞄前先由擁有人允許或展示的標籤，讓標籤在一般情況下不容易即時被掃瞄器閱讀；這樣的標籤在離開銷售點後仍可操作，同時對私隱會有更大保障。
- 在物品售出時，移除依附或內藏的標籤，停止標籤的功能，或給與消費者移除或停止標籤的選擇。
- 在 RFID 晶片內只儲存參考編號，而不是個人資料。
- RFID 標籤的使用，尤其會在物流情況以外下使用，須具透明度。
- 保護永久有效的 RFID 標籤免在當事人不知情下被隱蔽式閱讀器掃瞄。
- 需要時以加密方式保護必須留在產品上的資料。

Radio Frequency Identification (RFID) is an electronic tag that uses radio waves to transfer data to and from a reader. Typically, an RFID chip is used to memorise data and release it when queried by a non-contact reader for the purpose of tracking and identifying the object it is attached to. RFID chips have a variety of applications and are becoming popular and useful in the retail industry to better control the flow, replenishment and management of goods.

An RFID chip is often integrated in a product in a rather invisible way. Since such products are often used or carried by people, both the product and the individual become traceable without the knowledge of the individual.

The use of RFID tags presents certain privacy implications because of the following properties commonly found in most RFID chips: -

- **Always On**
  RFID tags cannot be switched off, as their power is often supplied by the reader remotely by radio wave. When a tag is placed near a reader, it is activated and its memory becomes available.
- **No Explicit Control**
  RFID tags automatically respond to a reader without the explicit "authorisation" of the individual carrying the tag, so RFID tags can operate and supply information without the individual's knowledge or consent.
- **Wireless Communication**
  It is relatively easy to read an RFID tag by a reader, and the tag-reader interaction is often invisible.

Hence, it is possible for someone to read from, or write to, an RFID tag without being noticed.

- **Open Standards**
  The majority of RFID tags for products carry an Electronic Product Code (EPC), which is a standard product code that allows anyone to easily look up the product the tag is attached to. It is therefore possible to use an RFID reader to scan and find out what a person is wearing or carrying, including the size and brand of clothes, medication package, book, etc. in order to understand the individual's health condition, personal preference etc.

It is important to note that RFID tags typically used for item labelling have a working range of 1 to 4 metres, so tags can be read from a relatively long distance. Coupled with the possible information stored in the chip (unique identifier, product information, etc.), if the chips are left on the purchased products after the point of sale, they pose the following privacy threats.

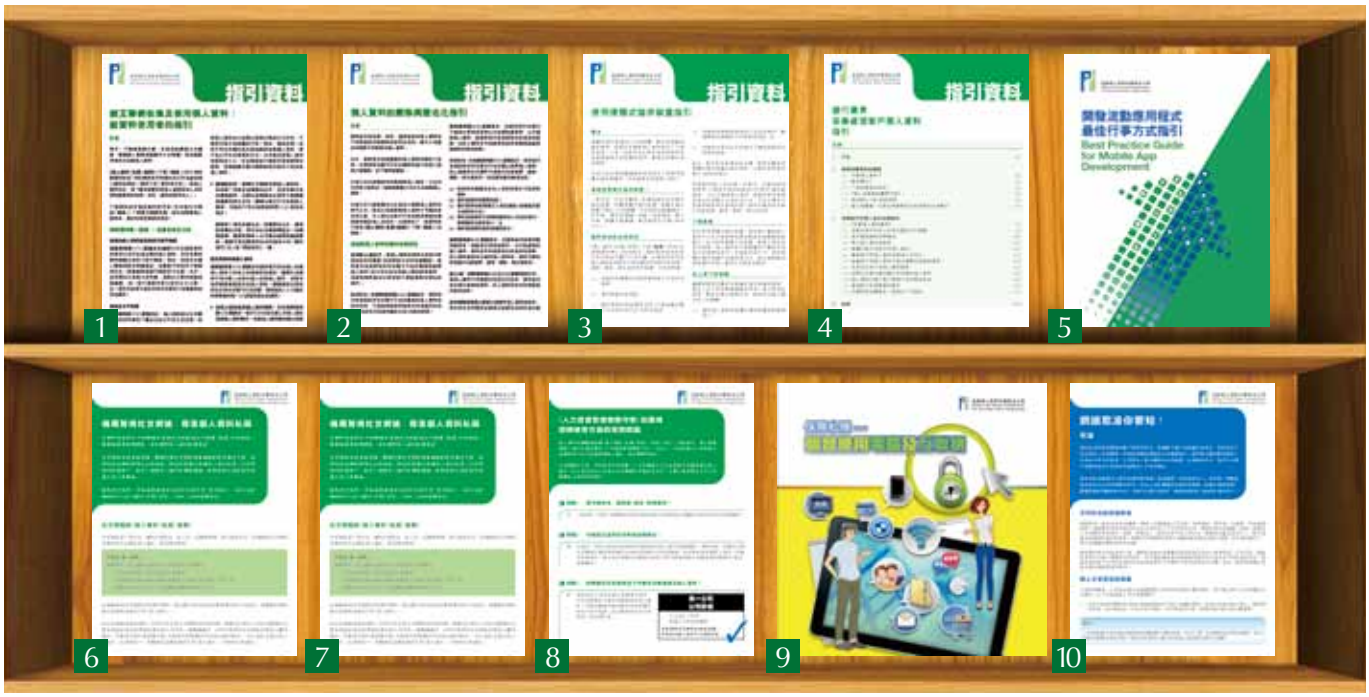
- **Position Traceability**
  Each tag has a unique manufacturing identifier. If it is possible to associate such an identifier to a specific person, it is also be possible to track the person's position by reading the tag on a T-shirt, for example, at different locations.
- **Information Leakage**
  It is possible to gather some information about people's belongings simply by reading the tags embedded in the items they carry, such as a passport, book, watch or medicine package. It would then be easy to further infer their personal preferences, health status or even political beliefs.

If no privacy impact assessment is carried out, RFID tags present possible privacy threats to consumers. The following countermeasures to prevent privacy abuse from the use of RFID tags, especially in the retail sector, are recommended.

- Design tags which are not easily readable by scanners in normal situations and have to be allowed or revealed by the owner of the objects before they can be scanned, so that tags can operate after the point of sale, while privacy is preserved.
- Disable or remove tags, or offer to consumer such choices, after the items they were attached to or embedded in are sold.
- Store a reference number instead of personal data on RFID chips.
- Be transparent about the use, particularly when the use is not limited to logistical controls, of RFID tags.
- Shield lifelong RFIDs against covert readers to avoid reading of tags without the knowledge of the owner.
- When appropriate, use encryption to protect information that must be left on merchandise.

資料來源 Sources：

"RFID Tag Privacy Threats and Countermeasures: Current Status", European Commission, Joint Research Centre – Institute for the Protection and Security of the Citizen
https://ec.europa.eu/jrc/sites/default/files/jrc78156_report_rfid_en.pdf



指引資料 Guidance Notes:

1 經互聯網收集及使用個人資料：給資料使用者的指引
Guidance for Data Users on the Collection and Use of Personal Data through the Internet

2 個人資料的刪除與匿名化指引
Guidance on Personal Data Erasure and Anonymisation

3 使用便攜式儲存裝置指引
Guidance on the Use of Portable Storage Devices

4 銀行業界妥善處理客戶個人資料指引
Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry

最佳行事方式指引 Best Practice Guide:

5 開發流動應用程式最佳行事方式指引
Best Practice Guide for Mobile App Development

資料單張 Information Leaflets:

6 機構智用社交網絡 尊重個人資料私隱
Privacy Implications for Organisational Use of Social Networks

7 網上行為追蹤
Online Behavioural Tracking

8 《人力資源管理實務守則》的應用 - 招聘廣告方面的常問問題
Understanding the Code of Practice on Human Resource Management - Frequently Asked Questions About Recruitment Advertisements

單張 Leaflets:

9 Protecting Privacy – Using Computers and the Internet Wisely
明智使用電腦及互聯網

10 Cyber-bullying – What you need to know
網絡欺凌你要知！

專員網誌 The Commissioner's Blog:

日期 Date	主題 Subject
2014	
04.29	Google Glass 和航拍機帶來的私隱挑戰 The Privacy Challenges of Google Glass and Drones
06.13	「私隱」並非止於「保障個人資料」 Privacy is more than personal data protection
06.26	互聯網的「被遺忘權」 Right to be forgotten
08.21	人對人直銷電話的拒收訊息登記冊 最終由哪一個政策局負責？ Renewed Call to Set Up a Do-not-call Register for Person-to-person Telemarketing Calls caught between two Bureaux

瀏覽電子版 View e-version:
www.pcpd.org.hk > 資源中心 > 刊物
www.pcpd.org.hk > Resources Centre > Publications

保障資料主任聯會
Data Protection Officers' Club

2014.12.22 午餐會系列：機構善用社交網絡 顧及保障個人資料
Lunch Talk Series: Optimising Social Networks for Business with Privacy Protection in Mind

www.pcpd.org.hk/dpoc

開發流動應用程式保障私隱活動
Privacy Campaign for Mobile Apps Development

2015.01.08 開展儀式暨研討會
Inaugural Ceremony cum Seminar

www.pcpd.org.hk/mobileapps

大學保障私隱活動 2014/15
University Privacy Campaign 2014/15

2015.01.23 講座：大學行政與私隱保障及資訊科技管理的資料保障
Seminars on Protecting Personal Data Privacy in University Administration and Data Protection in IT Management

www.pcpd.org.hk/university

保障個人資料巡迴展覽 2014/15
Public Education Roadshow on Personal Data Protection 2014/15

日期 Date	項目 Event	活動 Activities
2014.12.07, 12.14, 12. 28	2014/2015 年秋冬上環假日行人坊 Sheung Wan Promenade 2014/2015	攤位遊戲 booth game
2014.12.28 – 2015.01.10	流動展覽車巡迴港九新界各地 Roadshow across the city	展覽及互動遊戲 Exhibition and mini game

www.pcpd.org.hk/roadshow

其他教育及培訓項目：
Other Education & Training Programmes:

- 保障個人資料專業研習班
  Professional Workshops on Data Protection
- 《個人資料（私隱）條例》簡介講座（每兩星期舉行）
  "Introduction to the Personal Data (Privacy) Ordinance" Seminars (to be held bi-weekly)
- 保護個人資料私隱 – 日常生活與善用科技講座系列
  Protection of Personal Data Privacy – Talk Series on the Proper Use of Technology in Daily Life

詳情：**www.pcpd.org.hk > 教育及培訓**
Details: www.pcpd.org.hk > Education & Training

歡迎報名參加！
Join NOW!