

# Juris Doctor of the City University of Hong Kong

## Personal Data Protection in Hong Kong

### 8 April 2017



**Stephen Kai-yi Wong**  
**Privacy Commissioner for Personal Data, Hong Kong**

# Personal Data (Privacy) Ordinance

- Enacted in 1995
- Core provisions came into effect on 20 December 1996
- Personal Data (Privacy) (Amendment) Ordinance 2012 effective from 1 October 2012 except for “direct marketing” and “legal assistance” which took effect on 1 April 2013

# Limitations of Scope of Personal Data (Privacy) Ordinance

## Protection of Privacy Interests

- Information privacy ✓
- Territorial privacy ✗
- Personal privacy ✗
- Communications and surveillance privacy ✗

# What is personal data

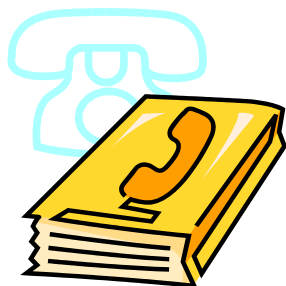
“**personal data**” (個人資料) means any **data** -

- (a) **relating** directly or indirectly to a living individual;
- (b) from which it is practicable for the **identity** of the individual to be directly or indirectly ascertained;  
and
- (c) in a **form** in which access to or processing of the data is practicable;

“**data**” (資料) means any representation of information (including an expression of opinion) **in any document**

# Examples of Personal Data used in everyday life

A person's name, mobile number, address, sex, age, occupation, salary, nationality, photo, identity card number, medical record, etc



# What is the meaning of the word “collect”?

## Eastweek Publisher vs PCPD



# What is the meaning of the word “collect”?

## Eastweek Publisher vs PCPD



### Case background

- The complainant was photographed by a magazine photographer without her knowledge or consent
- The photo was published in the magazine accompanied by unflattering and critical comments on her style of dress → caused embarrassment and inconvenience

### The Commissioner's decision

- Contravened the Ordinance on the grounds that the personal data of the complainant in the photograph was collected by unfair means

11

# What is the meaning of the word “collect”?

## Eastweek Publisher vs PCPD



### Actions taken by the magazine publisher:

- took the decision to the Court for judicial review and applied for an order of certiorari to quash the Commissioner’s decision
  - the judicial review held in the Court of First Instance and the judge dismissed the application
- appealed to the Court of Appeal
  - the Court of Appeal reversed the decision of the Court of First Instance and quashed the Commissioner’s finding of contravention

12



# What is the meaning of the word “collect”?

## Eastweek Publisher vs PCPD



### Ruling by the Court:

- In all the circumstances of the case, there had been no **“collection”** of personal data by the magazine publisher

### Meaning of “Collect”:

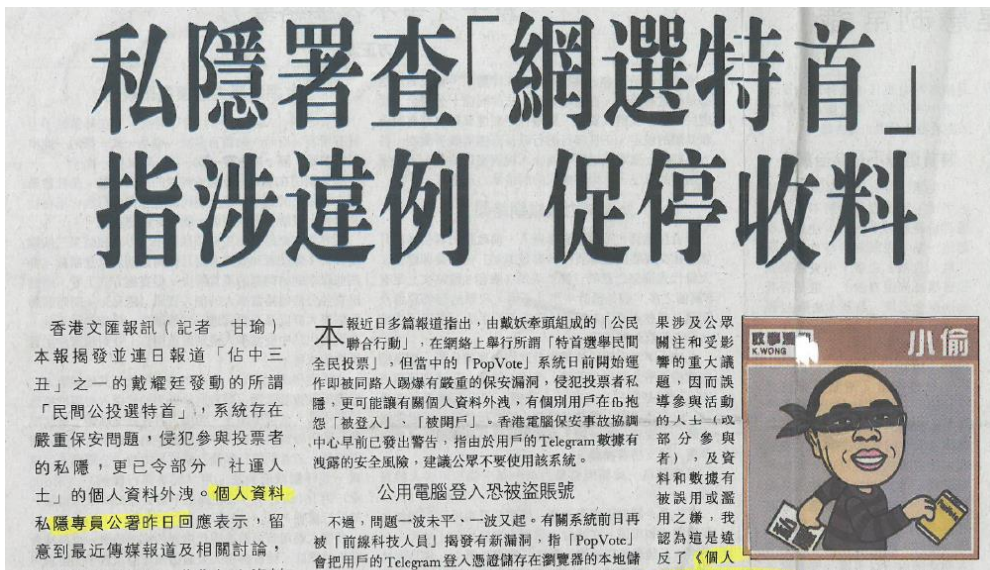
“... compiling information about an identified person or about a person whom the data user intends or seeks to identify”

“...the data collected relates to a subject whose identity is known or sought to be known by the data user as an **important item of information**”

**If no collection of personal data, the data protection principles would not be engaged at all**

13

# 「PopVote System」 may contravene the Principle of Fair Collection and had data security loopholes



Watchdog urges post-Occupy protesters stop collecting voters' personal data says may well be in contravention of

Danny Mak and Joyce Ng

Polytechnic for social public drawing security was launched

Organisers of an unofficial online poll on who should be the next chief executive have suspended their ballot after the privacy watchdog warned them it might be breaking the law.

Citizens United in Action, one of whose leaders is Occupy Central co-founder Benny Tai Yiu-ting, said it had halted the process until its members had spoken to Privacy Commissioner Stephen Wong Kai-ye.

"Although we have confidence in our system's security, we will

## 私隱署查公民提名涉濫用數據

【本報訊】「公民聯合行動」早前發起民間特首提名公投，已有逾1.4萬市民投票，但系統保安一直受批評，個人資料私隱專員公署昨晚發新聞稿，強烈要求PopVote立即停止不公平收集個人資料及使用有關Telegram通訊程式，並指已就事件展開循規審查。

截至昨午5時，4名主要特首參選人中，曾俊華以近8,000個提名領先，由民間團體及自派議員支持的梁國雄，以逾4,600個提名排第二，胡國興以約2,000個提名排第三，林鄭月娥及葉劉淑儀分別只有129及85個提名。

### 團體：將約見署方解釋

個人資料私隱專員公署昨晚發新聞稿，強烈要求PopVote立即停止不公平收集個人資料及使用有關Telegram通訊程式，公署稱活動無理據及無清楚說明收集個人資料目的和用途，資料和數據有被誤用或濫用之嫌，或違反《個人資料(私隱)條例》。

「公民聯合行動」昨晚發聲明回應，指會於日內主動約見公署，說明「公民聯合行動」透過是項活動收集個人資料的情況，包括收集目的、使用、保障個人私隱措施及資料保安安排，以釋除公署及公眾的疑慮。■記者余錦洪

# 「PopVote System」 may contravene the Principle of Fair Collection and had data security loopholes

## 私隱署指戴耀廷「特首民投」違例

本報早前率先報道，由佔中發起人戴耀廷發起的特首選舉公投計劃，存在私隱同保安風險，可能會令參加者嘅個人資料外洩。私隱專員公署尋日發表聲明，直指該計劃有誤導參加者同濫用其資料之嫌，違反《個人資料（私隱）條例》下嘅公平收集個人資料原則，強烈要求有關機構停止相關活動，參加者亦應停用相關嘅手機通訊程式。

### 涉誤導參加者 濫用資料

由戴耀廷發起的「公民聯合行動」，早前委託港大民意研究計劃及理大社會政策研究中心，舉辦「2017特首選舉民間全民投票」，大致係畀市民透過手機通訊程式，就各名特首參選人進

行公投；若某位或多位參選人取得一定票數，真正有權投票選特首嘅選舉委員會委員，就應該畀佢哋足夠嘅提名票，送佢哋「入閘」參選特首。

該計劃一推出，已有資訊科技專家同組織警告存在漏洞同風險，投票嘅個人資料可以輕易咁被還原同識別。私隱公署尋日更發表聲明，質疑計劃未有向參加者清楚

的、用途同有誤導參加料同數據可用。私隱專計劃違反公平收集原署已就事件循規審查。

■戴耀廷搞嘅被私隱署質疑濫用資料圖

## PopVote 暫停收集民間提名

【本報訊】由香港大學法律系副教授戴耀廷牽頭與多個民間團體組成的「公民聯合行動」，早前開始以PopVote普及投票系統進行「2017特首選舉民間投票」。不過，該投票系統一直被質疑存有保安風險，私隱專員公署前日強烈要求，PopVote普及投票系統立即停止不公平收集個人資料及使用有關Telegram通訊程式。

公民聯合行動昨日發表聲明，重申對普及投票系統的保安有信心，但為了減低

公眾的困擾，會暫停PopVote的網上收集提名。

### 曾俊華領先

公民聯合行動的聲明指已知悉私隱專員公署的關注，並表示會暫停PopVote普及投票系統的提名收集，直至與私隱專員取得聯絡，說明他們收集數據的用途，並明白私隱專員的要求後，才將系統重新開放。對於是次安排對市民造成不便，公民聯合

行動就事件向市民致歉。

網上提名系統暫停，明言要取得3.8萬公民提名去參選特首的社民連梁國雄，昨日繼續設置街站收集市民提名。截至昨日下午4時，一共有約1.6萬名市民透過PopVote普及投票系統投票，目前仍是由前財政司司長曾俊華領先，有8,146票，緊接的是社民連梁國雄及退休法官胡國興，二人分別有5,349及2,133票，而「大熱」林鄭月娥則只得133票。 ■記者陳雪玲

編輯：呂泳津 美術：陳小燕

# The online posting of passenger breastfeeding in back seat by a taxi driver

SOCIETY

## Outcry after taxi driver posts photo of breastfeeding mum

Police look into incident involving passengers as netizens condemn such disrespectful behaviour

Naomi Ng  
naomi.ng@smp.com

Police are looking into an incident in which a taxi driver posted online a secretly taken photo of a passenger feeding her baby.

Hong Kong's health minister also urged residents to respect breastfeeding mothers as the post triggered a public outcry.

The male driver posted the picture on a Facebook community group on Saturday with the caption: "Seriously, is this for real?"

The post, which has since been deleted, sparked a backlash from internet users, many of whom criticised him for what they said was disrespectful behaviour.

Police said they were looking into the incident and urged anyone with relevant information to contact them as soon as possible.

"The driver should not have intruded on someone's privacy in such a way, and should have respected the breastfeeding mother and given her space," Secretary for Food and Health Dr Ko Wing-man said yesterday.

He said it was important for Hongkongers to adopt the right attitude in understanding the needs of breastfeeding mothers, and that restaurants, shopping malls and public transport operators should show special consideration.

Jannie Leung Hoi-ting, chairwoman of the Hong Kong Breastfeeding Mothers' Association, said she hoped the incident would raise awareness of the difficulties faced by new mothers.

"When babies are hungry, they need to eat, so mothers should be able to breastfeed anywhere, any time. It's a very natural thing to do," Leung said.

**90**  
The number of corporations and restaurants that are backing breastfeeding facilities

In June, a ferry company launched the city's first breastfeeding station on public transport. More than 30 corporations and 60 restaurants across Hong Kong have pledged support for a campaign to provide breastfeeding facilities in offices and public spaces.

It is unclear how the taxi driver took the photo from the dashboard of the car. Some taxis in Hong Kong are equipped with closed-circuit television systems to resolve any disputes between drivers and passengers.

The cameras are part of a trial scheme to address complaints about poor service among some drivers, but have raised concerns over passenger privacy.

Drivers are required to notify passengers when they are entering a CCTV-equipped cab.

The Privacy Commissioner for Personal Data said it would not comment on individual cases, but believed the incident was a matter of personal conduct rather than being related to the implementation of the CCTV trial scheme.

The watchdog encouraged anyone who thought their personal data had been violated to make a complaint.

Anyone with information about the case can call police on 28605012.

5/11/14

## Cabbie drives into breastfeeding storm

Carain Yeung

Police are asking witnesses to step forward in an incident involving a taxi driver, who may have breached privacy laws by taking and uploading photos of a mother breastfeeding her baby inside his cab.



The taxi driver uploaded a video of a passenger breastfeeding her baby.

The pictures the driver, surnamed Chow, posted on Facebook early Saturday triggered a backlash. In the photos, a mother can be seen breastfeeding her baby, with her face and breasts clearly visible. Chow removed the photos after criticism from netizens, with some fellow taxi drivers calling him "a disgrace to the industry". The Police Cyber Security and Technology Crime Bureau is following up the incident and trying to locate the culprit driver.

Such incidents are rare in Hong Kong and police are studying relevant laws. "If members of the public have any information provide on the case, please contact the police promptly," a police spokesman said.

The Office of the Privacy Commissioner for Personal Data not comment on the case but called upon those who felt they had been invaded to lodge a complaint.

Collection and compilation of personal data fall under the Personal Data (Privacy) Ordinance and the privacy commissioner said the action was intentional, and the targeted person – the mother – can be identified, the spokesman added.

"It is disrespectful to personal privacy to film the breastfeeding process without the mother's consent," Secretary for Food and Health Ko Wing-man said yesterday. "He further trod on her privacy by distributing the information online."

Ko said the government has made efforts to promote breastfeeding in the past two years, with some shopping malls and public transport facilities having set up baby-care rooms, which are found in certain government departments.

But he admitted the government could do more.

## 司機上載的士客哺乳相 被轟無恥

安裝車廂攝錄無規管 議員促警方私隱署執法

主編推介

【明報專訊】一名自稱的士司機的網帖在社交網站貼出後，在士車乘客群組的圖片，全網引起轟動，更被指「唔啱嘢」，照片在網上流傳，要求大快刀裁員，其律師亦指，事件可能觸犯士車安裝攝錄無規管及侵犯私隱條例。

今年9月由香港警務處推行的士車安裝攝錄無規管，旨在加強對士車司機的監察，但引起不少乘客不滿，指其侵犯私隱。據悉，該名司機在車廂內安裝攝錄機，並在網上上傳其拍攝到的乘客哺乳的照片，引起網民強烈不滿。

警方表示，將調查該名司機是否違反了相關法律。此外，該名司機亦被指在車廂內安裝攝錄機，違反了相關規定。

該名司機表示，他是在車廂內安裝攝錄機，以便記錄乘客的投訴。他表示，他並沒有意識到自己的行為是錯誤的。

警方表示，將對該名司機進行調查，並視乎其行為的嚴重程度，決定是否對其採取法律行動。

此外，警方亦呼籲乘客在乘坐士車時，應注意車廂內的攝錄機，並可隨時向警方舉報。



車廂內哺乳

▲一名自稱的士司機的男子在facebook上，把乘客在車廂內哺乳的照片，全網引起轟動，更被指「唔啱嘢」。

【本報記者攝】

▲警方表示，將調查該名司機是否違反了相關法律。

【本報記者攝】

▲警方亦呼籲乘客在乘坐士車時，應注意車廂內的攝錄機。

【本報記者攝】

▲警方表示，將對該名司機進行調查。

【本報記者攝】

▲此外，警方亦呼籲乘客在乘坐士車時，應注意車廂內的攝錄機。

【本報記者攝】

▲警方表示，將對該名司機進行調查。

【本報記者攝】

▲此外，警方亦呼籲乘客在乘坐士車時，應注意車廂內的攝錄機。

【本報記者攝】

▲警方表示，將對該名司機進行調查。

【本報記者攝】

▲此外，警方亦呼籲乘客在乘坐士車時，應注意車廂內的攝錄機。

【本報記者攝】

▲警方表示，將對該名司機進行調查。

【本報記者攝】

▲此外，警方亦呼籲乘客在乘坐士車時，應注意車廂內的攝錄機。



車廂內哺乳

▲一名自稱的士司機的男子在facebook上，把乘客在車廂內哺乳的照片，全網引起轟動，更被指「唔啱嘢」。

【本報記者攝】

▲警方表示，將調查該名司機是否違反了相關法律。

【本報記者攝】

▲警方亦呼籲乘客在乘坐士車時，應注意車廂內的攝錄機。

【本報記者攝】

▲警方表示，將對該名司機進行調查。

【本報記者攝】

▲此外，警方亦呼籲乘客在乘坐士車時，應注意車廂內的攝錄機。

【本報記者攝】

▲警方表示，將對該名司機進行調查。

【本報記者攝】

▲此外，警方亦呼籲乘客在乘坐士車時，應注意車廂內的攝錄機。

【本報記者攝】

▲警方表示，將對該名司機進行調查。

【本報記者攝】

▲此外，警方亦呼籲乘客在乘坐士車時，應注意車廂內的攝錄機。

【本報記者攝】

▲警方表示，將對該名司機進行調查。

【本報記者攝】

▲此外，警方亦呼籲乘客在乘坐士車時，應注意車廂內的攝錄機。

PCPD 20 PCPD.org.hk est.1996

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

# The online posting of passerenger breastfeeding in back seat by a taxi driver

## 高永文轟不尊重私隱

# 警方跟進「的哥」偷拍餵母乳

有的士司機涉偷拍在車廂餵母乳的乘客，並將相片上傳互聯網，引發爭議。食物及衛生局局長高永文批評涉事司機不尊重私隱，指政府重解事件，呼籲市民提供資料。

高永文表示，不公開從私人途徑資料和照片，支持的士司機。



高永文對事件感到遺憾。



警方呼籲市民提供資料。

# 偷拍餵母乳放上網 全城譴責

## 行家批的哥「業界之恥」 警跟進籲市民報料

香港文匯報訊（記者杜若編）有的士司機涉偷拍女乘客在車廂內餵母乳，更將照片放上網公閱，事件引起全城譴責。網民紛紛留言，行家更指該名司機是「業界之恥」。事件已引起警方關注，據悉已交由網安及科技罪案調查科調查，並呼籲網民提供資料，食物及衛生局局長高永文亦表示，不公開從私人途徑資料和照片，支持的士司機。

高永文批不尊重母乳餵哺的權利，指其行為不尊重私隱。他表示，政府應加強對母乳餵哺的保護，並呼籲網民提供資料，協助警方調查。

【本報訊】一名外籍女子乘搭的士時，在車廂後座餵母乳，無意間被司機偷拍及把照片上傳上網，更把照片發到「唔都得」網民及婦女團體網頁，引起爭議。食物及衛生局局長高永文表示，不公開從私人途徑資料和照片，支持的士司機。

# 哺乳照 放上網 的哥被轟無恥



【本報訊】一名外籍女子乘搭的士時，在車廂後座餵母乳，無意間被司機偷拍及把照片上傳上網，更把照片發到「唔都得」網民及婦女團體網頁，引起爭議。食物及衛生局局長高永文表示，不公開從私人途徑資料和照片，支持的士司機。

警方對於此類事件表示關注，並呼籲網民提供資料，協助警方調查。此外，網安及科技罪案調查科亦表示，將對相關個案進行調查。

# Mobile apps with "call-blocking" function - collecting user's personal data

## APPS MAY HAVE YOUR NUMBER

Some three billion private telephone numbers have been compromised by call-filtering apps, including those of Chief Executive Leung Chun-ying and Chief Secretary Carrie Lam Cheng Yuet-ngor, FactWire reported.

The investigative news agency said three mobile apps for identifying spam calls – CM Security, Truecaller and Sync.Me – may breach privacy. They are suspected to have collected and integrated their users' contact list for a database, which allows app users to input a phone number to identify its owner.

Even those who did not download the apps are affected, as their identities could be revealed accidentally by their friends who have the apps and their contacts.

Results from FactWire's test showed Hong Kong's top two officials could be traced with their mobile number on Truecaller, a product of a US-listed company which main holding company is from China, and the Swedish-developed CM Security. Nearly all former and current lawmakers' mobile numbers also appeared on the two mobile apps.

Sync.Me, which is developed by an Israeli company, integrates the social media accounts to phone numbers, including IT-sector lawmaker Charles Mok, who has his mobile phone number merged with his Facebook, Google and LinkedIn profiles, the report said.

Such information of some other lawmakers, including Raymond Chan Chi-chuen, could be accessed only if app users pay a subscription. All three apps are free



The numbers of CY Leung and Carrie Lam can be traced on apps such as Truecaller.

to download from app stores and have been downloaded 200 million times.

Privacy Commissioner for Personal Data Stephen Wong Kai-yi said the watchdog will look into the matter if it has reasonable grounds to believe the apps have violated the law. But he said it will not comment on individual cases before understanding the apps and their operation.

Barrister Albert Luk Wai-hung told *The Standard* that users who unintentionally provide their friends' phone number may not have violated the law, as they did not do it on purpose.

He said the three app developers are unlikely to have violated the law, unless they put the data to other places which are not stated in the terms and conditions that require users' agreement when signing up for the apps.

Luk also said it may be difficult for the privacy watchdog to enforce the law, as the developers are not Hong Kong-based. YUPINA NG



「偽真名」作報章，由中國政府移動開發的手機應用程式CM Security、Truecaller及Sync.Me，獲傳的Truecaller及以色列的Sync.Me，指其會將用戶通訊錄轉移到雲端伺服器，整合成大量數據庫。其他人以成功向輸入號碼，即可在雲端獲得私人號碼，仍可查閱該號碼找到其身份。涉事程序至今在電腦已編碼完成。

據《偽真名》測試，發現香港多位名人包括部分高官、中聯辦官員、立法會議員及藝人的電話號碼，已被儲存於該數據庫。且Sync.Me更將手機號碼與社交媒體連結。只要有關號碼可供到持人的身份，Google等用戶，即可查閱該號碼與系統一格式，例如該號碼與該號碼被標記為「偽真名」，輸入該號碼將顯示為「偽真名」。

通訊錄上載雲端 科技界驚訝



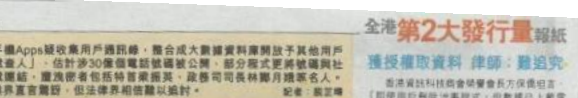
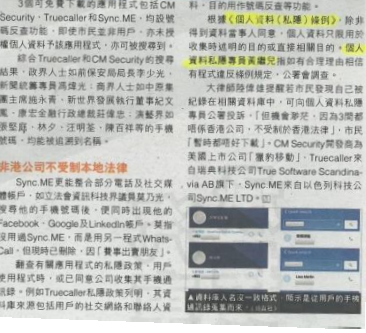
3個可免費下載的應用程式包括CM Security、Truecaller及Sync.Me，均被發現收集用戶通訊錄，即使市民並非用戶，亦未授權個人資料予該應用程式，亦可被搜尋到。

綜合Truecaller及CM Security的搜尋結果，政界人士如前政務司局長李卓人、新發展專員高煥光、商界人士如中聯辦專員陳志強、新世界發展執行董事紀宏業、康生金融行政總裁莊偉忠、港航界如張楚庭、林少、沈明暉、陳百祥等的手機號碼，均被搜尋到名稱。

非港公司不受本地法律

Sync.Me更整合部分電話及社交媒體號碼，如立法會議員科技界議員呂乃光，搜尋他的手機號碼後，便同時出現他的Facebook、Google及LinkedIn用戶。某網民用Sync.Me，而是用另一程式WhatsApp，但即時已顯示，「搜尋出實果」。

網民查詢有關程式的私隱政策，用戶使用程式時，就已同意公司收集其手機通訊錄。例如Truecaller公開聲明稱，其資料庫來源包括用戶的社交網絡和聯絡人



香港通訊科技協會會長黃方偉表示，「即使用戶刪除通訊錄，當數據上載雲端，資料仍會留存在伺服器」。

大律師樓律師樓，涉事開發商在要求用戶授權後才獲取資料，相信市民或可爭控，亦有律師，認為資料私隱政策應加強，非僅及事件，但程式亦大量收集通訊錄，會造成用戶資料被濫用及盜取，建議市民即時停用或更改聯絡者資料。

香港通訊科技協會會長黃方偉表示，「即使用戶刪除通訊錄，當數據上載雲端，資料仍會留存在伺服器」。

大律師樓律師樓，涉事開發商在要求用戶授權後才獲取資料，相信市民或可爭控，亦有律師，認為資料私隱政策應加強，非僅及事件，但程式亦大量收集通訊錄，會造成用戶資料被濫用及盜取，建議市民即時停用或更改聯絡者資料。



到多名政界人士的名稱，包括特首林鄭月娥、保安局局長李少光、新發展專員高煥光、中聯辦專員陳志強、香港6800萬市民保潔安潔、康生金融(1019)行政總裁莊偉忠及世界發展(1017)行政總裁紀宏業等。娛樂界人士則有張楚庭、沈明暉和陳百祥等。

程式資料庫的輸入人名稱格式，部分以羅馬顯示，如立法會議員呂乃光及陳志強分別為「[真名]」及「[Snow Bear]」。輸入人名稱以「[真名]」顯示，而通訊科技界人士則以「[真名]」顯示。

資料顯示，Truecaller收集全球超過30億個聯絡號碼，Sync.Me則收集了超過10億個聯絡號碼及社交媒體用戶。CM Security則透過其開發商公佈的聯絡號碼下另一手機通訊錄號碼，以被Truecaller及CM Security追蹤到名稱。

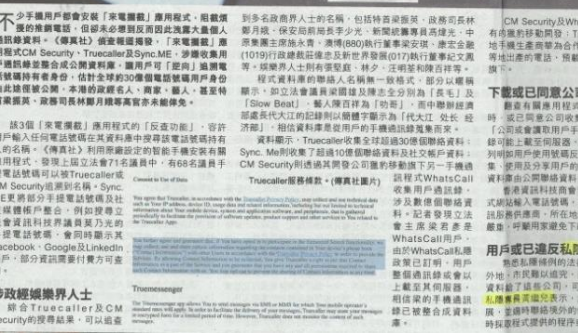
程式服務條款，(轉自社訊)

該應用程式提供「反打功能」，容許用戶輸入任何電話號碼在資料庫中查詢該電話號碼持有人的名稱。(轉自社訊)利用與該設計的智能手機安全有關應用程式，發現上述立法會71名議員中，有68名議員手機號碼號碼可以被Truecaller及CM Security追蹤到名稱。

Sync.Me更將部分非電話號碼及社交媒體號碼整合，例如搜尋立法會議員科技界議員呂乃光的手機號碼後，會同時顯示他的Facebook、Google及LinkedIn號碼，部分資訊需要付費才可查閱。

涉政號碼界人士

結合Truecaller及CM Security的搜尋結果，可以查



# Mainland mobile payment apps obtaining users' sensitive data

TECHNOLOGY

## Users' data at risk with major apps, report claims

Danny Lee and Nectar Gan

Mobile phone users' personal data and information is vulnerable to "misuse" and could be used for monitoring purposes by five of China's most popular mobile payment services, a news agency has reported.

Tencent's WeChat messaging app, the Alibaba Group's Taobao, Taobao World, Tmall and affiliate Alipay, which is run by Ant Financial, are all able to gain access to smartphones and collect sensitive information that could be transferred to the mainland, a FactWire investigation claimed yesterday.

The agency used programme analysis to examine how sensitive data was accessed by the apps, and tracked the information flow.

It showed the apps could

immediately, upon installation, obtain sensitive data that could track and identify a user, such as a smartphone's unique code and a SIM card's identification number.

The data was then recorded into files that were available for transfer to mainland servers, FactWire said.

Acquiring this information would allow one to access the

location of a device and track activities, such as software downloads or service visits, the agency claimed.

FactWire said it also tested Android Pay, Google Wallet and Octopus, and did not find the same results.

A Tencent spokeswoman told FactWire: "We take user data privacy and protection seriously in

product development and daily operations."

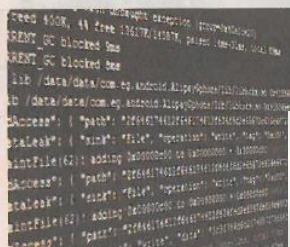
"WeChat will always adhere to Tencent's core mission to create value for our users by providing high standards of user experience and information security," the spokeswoman said.

Alibaba told the agency it complied with the law in collecting, storing and using information. It added that the collection of telephone numbers and SIM card information was needed to verify a user's identity and monetary transactions to combat fraud. Alibaba is the owner of the South

or regul transfer outside H

The f ment on apps had ever, a s public to of their a would be panies b

IT SE al Data which w data b Hong Kc



Payment apps including WeChat and T



2016.12.11 星期日

東方日報

港聞三 A24

用戶敏感資料傳內地 涉身份定位活動紀錄

### 五款支付Apps恐遭監控

港人近年不但愛透過手機購物，更愛以支付應用程式付款，但隨時引發隱私危機。有報道指五款由內地公司開發的熱門網絡支付應用程式，包括WeChat、淘寶、淘寶全球、支付寶錢包及天貓，除可識別用戶身份、記錄活動及位置定位等敏感資料，更可能把相關資料隨時傳送到內地的伺服器。有電腦專家指，相關敏感資料接收後，用戶在手機的一舉一動，都可能會被追蹤、監視或盜取。

傳訊社早前使用靜態程式分析，發現上述五款支付應用程式，即可讀取多項敏感資料，包括「用戶識別碼設備識別碼」(IMEI)、「國際移動用戶識別碼」(IMSI)、「SIM卡識別碼」(ICCID)、「電話號碼」電話號碼及對方電話號碼等，亦可取得管理或使用者、存取位置及錄音功能。

該社亦用動態程式分析進一步分析，結果顯示，五款支付應用程式已將用戶的IMEI、ICCID、IMSI等資料傳送到內地的伺服器。相見，該社同時測試另外三個網上交易應用程式，包括Android Pay、Google Wallet及八達通，顯示均未存取IMEI、IMSI等敏感資料。

該社引述中文大學信息工程學系助理教授倪克堯表示，IMEI、IMSI等資料是辨識敏感資料，可取得手機定位資料，如簡介人住家系統，實際上可以跟蹤用戶電話。如高ICCID，用戶在手機中的一舉一動，都可能會被追蹤、監視或盜取，其實非常危險。

理工大學電子計算學系副教授陳志輝向本報表示，不論內地支付應用程式的保安

東方日報

港聞三 A24

用戶敏感資料傳內地 涉身份定位活動紀錄

五款支付Apps恐遭監控

但指手機好比電腦，支付應用程式與電腦程式無異，敏感資料雖有機外洩，由於外間如美國較重隱私，故程式有很多限制，無法讀取太多資料作其他用途。

他又指，除支付應用程式，其他手機應用程式或沒有全數定位客戶的電子錢包，亦有機會儲存所在位置，連繫每日生活模式。若底人不法之徒手中，復非不潔思想，市民應審慎決定是否下載或使用。

阿里巴巴：依法收集訊息

阿里巴巴集團淘寶、淘寶全球及天貓網零售巨擘指出，對訊息的收集、儲存和使用均遵守法律規程，高度重視用戶信息保護。網購金服支付寶錢包表示，用戶支付寶錢包收IMEI、IMSI數據，是保障用戶的帳戶安全。

香港個人資料私隱專員公署表示，(個人資料(私隱)條例)並無境外法律效力，該署不會評論任何國家或司法管轄區的法例或規定。

## 五款內地Apps 或助政府監控

# 淘寶 微信 洩用戶私隱



【本報訊】繼手機「來電攔截」應用程式洩露全球數十億人電話資料後，再有手機程式出現嚴重隱患。據傳真社(FactWire)調查報道，港人常用的五款內地通訊或網購應用程式(Apps)包括淘寶、微信(WeChat)、淘寶全球、支付寶錢包及天貓，紀錄用戶活動及位置等資料並存取成檔案，再抄送回內地伺服器。

記者：伍婉文

上述5種應用程式分別由騰訊(700)及阿里巴巴營運，傳真社記者經測試發現用戶下載程式後，開發商可取得「讀取手機狀態及識別碼」權限，即手機識別碼(IMEI)、電話號碼及裝置所屬號碼(IMSI)、SIM Card編號(ICCID)、電話號碼及通話資料等；又把資料存檔後送回內地伺服器。報道只測試了Android系統手機，沒有iOS系統手機。報道又以惡意軟件分析服務VirusTotal檢查，發現支付寶安裝有木馬程式Android Trojan SMS Spy，可截取手機的SMS短訊，淘寶亦也有一個backdoor.androidos.ginmaster程式，盜取用戶資訊。

個人資料私隱專員公署指，香港無法禁止個人資料傳送至香港以外的地方。阿里巴巴回覆查詢指，公司收集、儲存和使用用戶訊息均遵守適用法規。螞蟥金服就支付寶錢包回覆指，得到用戶授權後收集IMEI、IMSI數據，是為了更好保障用戶帳戶安全。WeChat回覆指，公司及旗下網站前年1月取得環球Truste認證，致力保障用戶私隱和資料。

# Suspected data leakage by an airline's mobile app



**Book Flight**

Type:  Round Trip  One-way  Stopover/Multi-city

From:

To:

Departure Date: 2017-01-23

Return Date: 2017-01-26

Cabin: Economy

Adult (Aged 12 or above): 1

Child (2-11 years): 0

Payment: Hong Kong Dollar HKD

**Search**

**Book Hotel**

**Flight Status**

Home > Special News

**Special News**

**Hong Kong Airlines Statement Regarding Mobile APP**  
Last Updated:(Hong Kong)2017-01-03

Hong Kong Airlines (the "Company") is actively investigating a recent case of leakage information from Hong Kong Airlines mobile APP (the "APP"). Immediate remedial action taken to suspend the non-member customers using Android system from conducting a and booking information enquiry via the APP. The Company has engaged a third party to inquire into this situation, aiming to find a comprehensive solution that will prevent re-occurrence. The Company has also reported the case to the Office of the Privacy Commissioner for Personal Data (PCPD).

Only non-member customers using a few mobile phone brands installed with Android system (6.0 or above) via the APP are potentially affected in this incident. The problem only exists on these mobile phone brands and does not affect Hong Kong Airlines official website or mobile website. Based on our investigation, 57 customers were affected in this incident.

Hong Kong Airlines attaches great importance to the personal privacy of its customers and sincerely apologizes for the inconvenience that may cause to the immediate actions to prevent further leakage and recurrence.

Please refer to the Frequently Asked Questions below for further information.

- How do I know if I am one of the affected party?**  
Based on our preliminary investigation, we have identified 57 affected customers using a few mobile phone brands installed with Android system. The APP are potentially affected in this incident. We will contact you if you are one of the affected customers. If you are concerned whether you are an affected customer, please contact our dedicated email address at [app.enquiry@hkairlines.com](mailto:app.enquiry@hkairlines.com).
- What data might have been leaked in this incident?**  
As of now, the known affected data includes passenger name, name of the flight, email (if applicable), ticket number, ID or travel document number, online check-in status and QR code of the boarding pass. Please rest assured that the payment details of customers including credit card information and bank account information have NOT been affected.



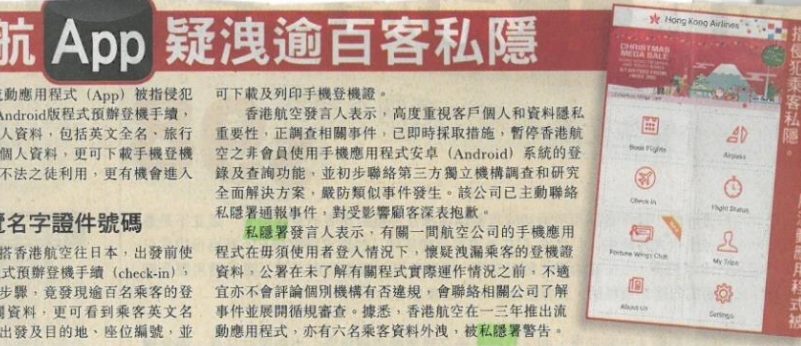
**【本報訊】**香港航空的手機應用程式(App)3年內第二度洩漏客戶私隱。《蘋果》發現推款 Android 版程式早期錯誤洩漏數以百計乘客機位紀錄、外洩私隱資料包括客人大英文全名、營業種航線資料以及旅行證件號碼。不法者可藉此下載登機證資料來客，對機位保安構成威脅，私隱專員公署稱會對事件展開調查。

記者：周子祥 區佩儀

香港航空最近向媒體承認，其三年前推出的 Android 版機位查詢應用程式，存在嚴重安全漏洞，導致數以百計乘客的個人資料外洩。據悉，該應用程式在設計上存在缺陷，未能對用戶身份進行嚴格驗證，致使不法分子能夠輕易獲取乘客的機位信息、姓名、電話號碼等敏感數據。此外，該程式還洩露了航空公司的內部運營數據，包括航線、班期及票價等。這一事件引起了社會的廣泛關注，並引發了對航空公司數據安全的質疑。

香港航空發言人表示，公司在發現問題後立即採取了緊急措施，包括停止該應用程式的運行，並對受影響的數據進行了封存。目前，公司正與專業安全團隊合作，對漏洞進行徹底排查，並尋求長期的解決方案。同時，公司也對受影響的乘客表示誠摯的歉意，並承諾將採取一切必要措施，確保客戶的個人信息安全。

私隱專員公署表示，將對此次事件展開調查，以確定是否存在違規行為，並對相關責任進行追究。公署呼籲航空公司應加強數據安全管理，定期進行安全評估，並提高員工的安全意識，以預防類似事件的再次發生。



**【本報訊】**香港航空有流動應用程式 (App) 被指洩漏乘客私隱，有市民利用港航 Android 版程式預辦登機手續，竟發現逾百名其他乘客的個人資料，包括英文全名、旅行證件號碼等，若再輸入上述個人資料，更可下載手機登機證。除引發私隱危機，若被不法之徒利用，更有機會進入機場禁區，後果不堪設想。

**預辦登機飽覽名字證件號碼**

據悉，有市民上月底乘搭香港航空往日本，出發前使用港航 Android 版流動應用程式預辦登機手續 (check-in)，以訪客身份進入，經過四個步驟，竟發現逾百名乘客的登機紀錄，再進一步輸入相關資料，更可看到乘客英文名字、證件號碼、飛行日期、出發及目的地、座位編號，並可下載及列印手機登機證。

香港航空發言人表示，高度重視客戶個人和資料私隱重要性，正調查相關事件，已即時採取措施，暫停香港航空之非會員使用手機應用程式 Android (Android) 系統的登錄及查詢功能，並初步聯絡第三方獨立機構調查和尋求全面解決方案，嚴防類似事件發生。該公司已主動聯絡私隱專員公署，對受影響乘客深表抱歉。

私隱專員發言人表示，有關一間航空公司的手機應用程式在毋須使用者登入情況下，懷疑洩漏乘客的登機證資料，公署在未了解有關程式實際運作情況之前，不適宜亦不會評論個別機構有否違規，會聯絡相關公司了解事件並展開覆核調查。據悉，香港航空在一年內推出流動應用程式，亦有六名乘客資料外洩，被私隱專員警告。



# CCTV installation at Refuse Deposit Blackspots

## CCTV to zoom in on scourge of illegal dumping in Hong Kong

Black spots near restaurants will be monitored in pilot scheme to stamp out poor hygiene conditions

PUBLISHED : Tuesday, 20 September, 2016, 11:32pm  
UPDATED : Wednesday, 21 September, 2016, 12:09pm

COMMENTS : 5



Elizabeth Cheung

12 SHARES



More on this story



HEALTH & ENVIRONMENT

CCTV will be installed at black spots under a pilot scheme in the fight against the illegal dumping of rubbish.

The measure, to be launched by the end of this year, aims to curb poor hygiene conditions in areas such as back alleys close to restaurants.

Secretary for Food and Health Dr Kwok Ka-kit hopes the installation of closed-circuit TV will help enforce the law.

"Rubbish may not be dumped at daytime in these areas. It was reported that dumping of rubbish from homes or restaurants at inappropriate locations may happen at midnight," he said yesterday after meeting the chairmen and vice chairmen of district council food and environmental hygiene committees.

The 18 councils will be asked to identify hygiene black spots requiring further surveillance.

The pilot scheme is expected to last from six months to a year.

When asked about privacy concerns, health officials said guidelines on CCTV surveillance issued by the Office of the Privacy Commissioner would be followed.

"If the installation involves external walls of private buildings, we will seek consent from the owners' corporations or owners of the buildings before proceeding," Vivian Lau Lee-kwan, director of food and environmental hygiene, said.

## 中環深水埗元朗 裝CCTV捉垃圾蟲

【本報訊】為打擊垃圾蟲，食環署將在下周五（30日）起在中西區、深水埗區、元朗區6個垃圾黑點各啟用兩部網絡攝錄機（CCTV），密切監察目標、策劃檢控行動，計劃有關會拓展至全港。人權組織指，亂掉垃圾屬低度清潔問題，毋須用保護方法處理，憂慮錄像被濫用，長遠僅對市民私隱、立法會議員指，中西區裝置地點並非傳統垃圾黑點，相信增加區人手通宵「捉垃圾蟲」會更有力。

食環署指，12月30日將推行網絡攝錄機試驗計劃，打擊個別地區的衛生問題。安裝攝錄機的地點包括中環、深水埗及元朗，6個地點各安裝2部網絡攝錄機，食環署將與區議會密切合作，策劃執法、計劃會由垃圾攝錄機6個月後檢討。

食環署稱，將在攝影範圍內貼告示，亦會要求員工嚴守《個人資料（私隱）條例》第496條的規定，毋得將錄像用於監察或執法行動。有關事項在六個月內未獲檢控，將關閉攝錄機。

人權監察對食環署又指，政府昨日多次提出在中環特許等處安裝攝錄機監視電視，惟不少處非屬影響衛生黑點範圍，指認為網絡攝錄機仍對私隱有影響，不明白為何低度的清潔問題，要用保護市民方式處理。

據悉，攝錄機24小時運作，但錄影的人員，由政府有經驗警務人員操作（14日）被宣佈，安裝人員好幾日，而適用於本報的《個人資料條例》已明，市民私隱受保障。

實施日期	每月30日(五)
實施地點	中西區、深水埗區、元朗區
地點	中環士丹利街2-4號已離業華會會館及必列者士街(前城皇街)垃圾收集站及元朗東堤街垃圾收集站及十八鄉白沙村垃圾收集站
攝錄機	各點攝錄機
攝錄機用途	監察垃圾蟲、監察非法傾倒、非法傾倒垃圾、監察非法傾倒、非法傾倒垃圾
攝錄機數量	每點攝錄機2部

## 蘇豪區堆積垃圾「執機都有」

【本報訊】試行期間監察起見，食環署將在中環、深水埗及元朗區6個地點，分別安裝兩部網絡攝錄機，密切監察目標、策劃檢控行動，計劃有關會拓展至全港。人權組織指，亂掉垃圾屬低度清潔問題，毋須用保護方法處理，憂慮錄像被濫用，長遠僅對市民私隱、立法會議員指，中西區裝置地點並非傳統垃圾黑點，相信增加區人手通宵「捉垃圾蟲」會更有力。

食環署指，12月30日將推行網絡攝錄機試驗計劃，打擊個別地區的衛生問題。安裝攝錄機的地點包括中環、深水埗及元朗，6個地點各安裝2部網絡攝錄機，食環署將與區議會密切合作，策劃執法、計劃會由垃圾攝錄機6個月後檢討。

食環署稱，將在攝影範圍內貼告示，亦會要求員工嚴守《個人資料（私隱）條例》第496條的規定，毋得將錄像用於監察或執法行動。有關事項在六個月內未獲檢控，將關閉攝錄機。

人權監察對食環署又指，政府昨日多次提出在中環特許等處安裝攝錄機監視電視，惟不少處非屬影響衛生黑點範圍，指認為網絡攝錄機仍對私隱有影響，不明白為何低度的清潔問題，要用保護市民方式處理。

據悉，攝錄機24小時運作，但錄影的人員，由政府有經驗警務人員操作（14日）被宣佈，安裝人員好幾日，而適用於本報的《個人資料條例》已明，市民私隱受保障。

## 六棄置垃圾黑點 食環署裝攝錄機

食環署本月三十日(下周五)起在中西區、深水埗區及元朗區共六個棄置垃圾黑點展開網絡攝錄機試驗計劃，加強監察違例棄置垃圾情況及策劃執法行動。

## 試驗六個月後檢討

該六個棄置垃圾黑點，包括中環士丹利街2-4號已離業華會會館側巷及必列者士街(前城皇街)垃圾收集站附近；深水埗連翔道南行避車處及昌華街垃圾收集站；以及元朗東堤街垃圾收集站及十八鄉白沙村垃圾收集站，各安裝兩部網絡攝錄機。

食環署指，該些衛生黑點經常被人棄置垃圾和廢物，特別在午夜或清晨時分，引致環境衛生問題。署方已就試驗計劃徵詢相關區議會意見得到支持，六個月後作檢討。署方會根據個人資料私隱專員公署發出的「閉路電視監察措施指引」，在攝錄範圍內張貼告示，以示網絡攝錄機正運作。所有錄像只用於法律行動上需要，若違例事項在六個月內未作檢控，有關錄像將刪除。

# The Six Data Protection Principles (DPPs)

## 6 保障資料原則 Data Protection Principles

PCPD.org.hk

### 1 收集目的及方式 Collection Purpose & Means



資料使用者須以合法和公平的方式，收集他人的個人資料，其目的應直接與其職能或活動有關。  
須以切實可行的方法告知資料當事人收集其個人資料的目的，以及資料可能會被轉移給哪類人士。  
收集的資料是有實際需要的，而不超乎速度。

Personal data must be collected in a lawful and fair way, for a purpose directly related to a function/activity of the data user.  
All practicable steps shall be taken to notify the data subjects of the purpose of data collection, and the classes of persons to whom the data may be transferred.  
Data collected should be necessary but not excessive.

### 2 準確性儲存及保留 Accuracy & Retention



資料使用者須確保持有的個人資料準確無誤，資料的保留時間不應超過達成原來目的實際所需。

Personal data is accurate and is not kept for a period longer than is necessary to fulfill the purpose for which it is used.

### 3 使用 Use



個人資料只限用於收集時述明的目的或直接相關的目的，除非得到資料當事人自願和明確的同意。

Personal data is used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent is obtained from the data subject.

### 4 保安措施 Security



資料使用者須採取切實可行的步驟，保障個人資料不會未經授權或意外地被查閱、處理、刪除、喪失或使用。

A data user needs to take practical steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.

### 5 透明度 Openness



資料使用者須公開其處理個人資料的政策和行事方式，交代其持有的個人資料類別和用途。

A data user must make known to the public its personal data policies and practices, types of personal data it holds and how the data is used.

### 6 查閱及更正 Data Access & Correction



資料當事人有權要求查閱其個人資料；若發現有關個人資料不準確，有權要求更正。

A data subject must be given access to his personal data and to make corrections where the data is inaccurate.

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

# Six Data Protection Principles Introduction Video

《 個人資料(私隱)條例 》下的

## 六項保障資料原則

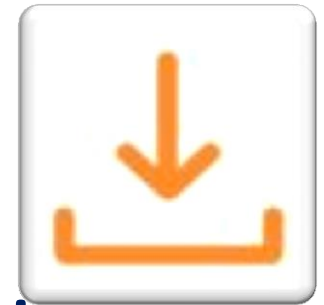
Six Data Protection Principles under the Ordinance



23

# Principle 1 – Purpose and Manner of Collection

- must be related to the data user's functions or activities
- data collected should be adequate but not excessive
- the means of collection must be lawful and fair
- all practicable steps to notify data subjects of collection purposes and to whom data will be transferred (i.e. provision of personal information collection statement "PICS")



# Principle 1 – Purpose and Manner of Collection

## Case Sharing: Face Magazine Limited and Sudden Weekly Limited (AAB No.5 & 6/2012)


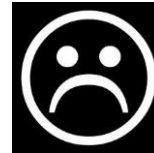
- The photos of three artistes were captured by the adoption of systematic surveillance and use of long lens cameras
- The photos were published in two magazines depicting the daily life of the artistes and their intimate acts suggesting of their cohabitation
- The artistes were at their respective places of residence which were not easily visible to the public
- The artistes had a reasonable expectation of privacy in the circumstances

# Principle 1 – Purpose and Manner of Collection

- The public interest is one factor to be considered as to whether or not the collection of personal data is fair in the circumstances. It is a question of balancing the fairness in collecting the personal data against the public interest in knowing the truth
- What the appellants sought to expose (namely, cohabitation between the artistes) was not in the public interest
- Contravention of **the Principle of Fair Collection**

# Personal Information Collection Statement

- ill-defined purposes of use



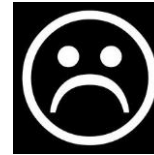
- .....
- Other related purposes
- .....





- If you provide any personal data to us, you agree that we can use personal data about you for any purpose we choose

# Personal Information Collection Statement

- ill-defined data transferees



- 
- any other persons under a duty of confidentiality to our company

- 
- any company within our Group, our respective subsidiaries and any company in which the same has an interest



# Personal Information Collection Statement

## Practical tips:



design the layout of PICS (including font size, spacing and use of appropriate highlights) in an easily readable manner



present PICS in a conspicuous manner, e.g. in a stand-alone notice or section



use reader friendly language, e.g. simple words



provide further assistance to customers such as help desk or enquiry service



should not state the purpose of use and class of transferees in general and vague terms

## Principle 2 – Accuracy and duration of retention

- data users shall take all practicable steps to ensure the accuracy of personal data held by them, and destroy data after the purpose of use is fulfilled



# Principle 2 – Accuracy and duration of retention

**Case Sharing: bank statements sent to inaccurate customer address causing disclosure of personal data to unintended recipient**

- credit card customer provided address in “Shek Tong Tsui”
- bank statement delivered to “Siu Lam”
- complainant used bank’s form to correct the address
- bank subsequently sent statements to an address in Shek Tong Tsui, but without specifying the flat number



# Principle 2 – Accuracy and duration of retention

- bank's double-checking procedures failed to spot the mistakes
- contravention of **Principle 2**
- the Commissioner issued enforcement notice to the bank directing it to conduct regular administrative audit for customers' requests to update personal data



# Principle 2 – Accuracy and duration of retention

- **Case Sharing: Inland Revenue Department (IRD) Failed to Take All Reasonably Practicable Steps to Ensure the Accuracy of a Taxpayer’s Address**
  - **Failing to receive Tax Demand despite calls and emails were sent to clarify address**
  - **Officer A of IRD wrongly attached the Appendix of another taxpayer to the Main Return of the Complainant; Officer B updated IRD database without checking the file numbers on the Appendix and Main Return; Tax Demand sent to wrong address and returned undelivered; Officer C attempted to rectify by checking the tax return of Complainant’s employer but wrongly input “Flat A” instead of “Flat F”**

# Principle 2 – Accuracy and duration of retention

- After receipt of Complainant's enquiry emails, Officer D simply instructed subordinate to resend copies of Tax Demand according to database, as many as three times
- Remedial actions – revise Tax Return to incorporate address change into the Main Return; daily supervisory checking on at least 10% of address amendments

# Principle 2 – Accuracy and duration of retention

Accuracy of the data may not be apparent or easily determined in some cases

- The Complainant was diagnosed as having “serious psychosis” by a psychiatry clinic of the Hospital Authority (“HA”), and he later sought consultation at a private clinic and was diagnosed as having “anxiety disorder”. He then lodged a complaint with the PCPD against the HA for holding inaccurate medical records about him.
- **No** contravention of DPP2
- According to the Administrative Appeals Board, medical opinions about judgment of the mental condition of a data subject were the professional judgment of the doctor, and its accuracy was not within the jurisdiction of the Ordinance or the PCPD and the Commissioner could not compel the doctor to amend his medical opinion

# Principle 2 – Accuracy and duration of retention

**Case Sharing: an insurance company retained personal data of unsuccessful insurance applicants for indefinite period of time**

- reasons given by insurer
  - legal requirements for keeping books of accounts
  - guidelines and circulars of regulatory authorities
  - potential litigations, enquiries and complaints
  - checking against future applications





# Principle 2 – Accuracy and duration of retention

- **Privacy Commissioner’s decision:**
  - ❖ **monetary transaction – retain 7 years**
  - ❖ **non-monetary transaction – retain 2 years**
  - ❖ **unless special circumstances existed**
- **insurer complied with the enforcement notice issued by the Commissioner, and erased more than 7,000 records**



## Principle 3 – Use of personal data

- personal data shall not, without the prescribed consent of the data subject, be used for a new purpose

*“new purpose” means any purpose other than the purposes for which they were collected or directly related purposes*



# DPP 3 – Use of personal data

## Case sharing: Use of Group Instant Messaging App

- MPF intermediary added a customer to his WhatsApp group for circulating MPF related information
- thereby disclosed the customer's name and mobile number to members of the group
- no consent from customer
- contravention of **DPP3**



# Principle 4 – Security of personal data

- data users shall take all practicable steps, to safeguard personal data against unauthorised or accidental access, processing, erasure, loss or use



# Principle 4 – Security of personal data

Case Sharing: a bank failed to safeguard the personal data collected during an outside-office marketing campaign

- bank conducted a marketing campaign in a bookshop to solicit credit card applications
- after work, bank's employee put all application forms and identity card copies in a briefcase and carried them home
- the employee left briefcase in a public light bus and lost all the documents
- bank did not have adequate guidelines to staff for handling personal data collected during outside-office marketing campaigns
- **breach of Principle 4**
- enforcement notice issued to the bank and remedial actions taken (e.g. transfer documents to a nearby branch immediately after work)



# Principle 5 – Information to be generally available

**Data users shall provide:**

- (a) policies and practices in relation to handling of personal data;**
- (b) the kinds of personal data held;**
- (c) the main purposes for which personal data are used**



42

## Principle 6 – Access to personal data

- data subject is entitled to request access to and correction of his personal data
- data user may charge a non-excessive fee
- data user shall respond within 40 days



# Application of exemption

- After work injury, the Complainant, a technician of a public transport institution, was referred to psychological treatment during which the Complainant had told the psychologist and counsellor of a service association more than once that he wanted to blow up the public transport facilities of the institution (“the Data”). After consideration and discussion with the psychologist, the association informed the institution of the Data
- The PCPD considers that blowing up public transport facilities is unlawful or seriously improper conduct under section 58(1)(d) of the Ordinance. The association informed the institution of the Data for the prevention of the above conduct. Under the circumstances, the Data should be exempt from the requirement



# Application of exemption

- Moreover, the Data was also the personal data relating to the physical or mental health of the technician under section 59 of the Ordinance. If the association could not disclose the Data without the consent of the technician, it would be likely to cause serious harm to the physical or mental health of the technician. Under the circumstances, the Data should also be exempt from the requirement

# Direct Marketing



# Direct Marketing Requirements

- The new provisions on regulation of direct marketing activities came into force on 1 April 2013
- direct marketing activities under the Ordinance include such activities made to *specific persons* by mail, fax, email and phone



# Examples of Non-Direct Marketing Activities

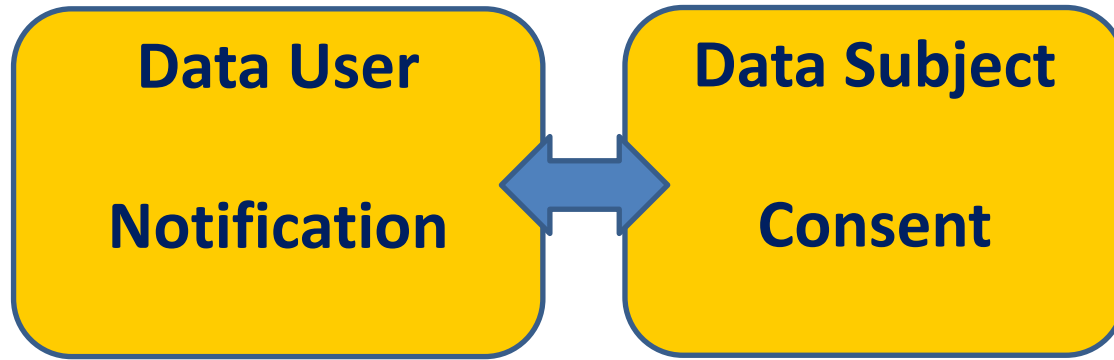
## Unsolicited Electronic Messages



Unsolicited Electronic Messages Ordinance

# Direct Marketing Requirements

Intends to use or provide personal data to others for direct marketing



Provides personal data

<ul style="list-style-type: none"><li>• provide “prescribed information” and response channel for data subjects to elect whether to give consent</li><li>• notification must be easily understandable</li></ul>	<ul style="list-style-type: none"><li>• consent should be given explicitly and voluntarily</li><li>• “consent” includes an indication of “no objection”</li></ul>
---	---

# Direct Marketing Requirements

- if a data subject submits an opt-out request, the data user must comply with the request without charge



# Direct Marketing Conviction Cases

Date	Case	Penalty
Sep 2015	A telecommunication company ignored customer's opt-out requests	Fined \$30,000
Sep 2015	A storage service provider failed to take specified actions and obtain the data subject's consent before direct marketing	Fined \$10,000
Nov 2015	A healthcare services company ignored customer's opt-out requests	Fined \$10,000
Dec 2015 <i>(Note: Appeal trial in progress)</i>	An individual provided personal data to a third party for direct marketing without taking specified actions and obtaining the data subject's consent	Fined \$5,000
Apr 2016	<ul style="list-style-type: none"> <li>An insurance agent used personal data for direct marketing without taking specified actions and obtain the data subject's consent; and</li> <li>Failed to inform the data subject of his opt-out right when using his personal data in direct marketing for the first time</li> </ul>	Community Service Order of 80 hours for each charge

51

# Direct Marketing Conviction Cases

Date	Case	Penalty
May 2016	<ul style="list-style-type: none"> <li>• a telemarketing company used a customer's personal data in direct marketing without taking specified actions and obtaining his consent; and</li> <li>• ignored opt-out requests</li> </ul>	Fined \$8,000 for each charge
Dec 2016	<ul style="list-style-type: none"> <li>• a watch company used personal data for direct marketing without taking specified actions and obtain the data subject's consent; and</li> <li>• failed to inform the data subject of his opt-out right when using his personal data in direct marketing for the first time</li> </ul>	Fined \$8,000 for each charge
Jan 2017	<ul style="list-style-type: none"> <li>• A bank ignored customer's opt-out requests</li> </ul>	Fined \$10,000



# Practical Tips



**must take specified actions and obtain consent**



**must notify data subject of his opt-out right**



**update the Opt-Out List timely**



**ensure that staff follow standing procedures**

# Consequences of Breach



- Investigation and Enforcement by PCPD
  - After investigation, publish a report (**section 48**) – naming the relevant data user
  - Serve an enforcement notice (執行通知) on the relevant data user (**section 50**) – non compliance with an enforcement notice or repeated contravention by the same act is a criminal offence (**section 50A**)

# Consequences of Breach

- Complainant has right of appeal to the AAB against
  - Commissioner's refusal not to carry out or decision to terminate an investigation (**section 39(4)**)
  - Commissioner's decision not to serve an enforcement notice in consequence of an investigation (**section 47(4)**)
- Data user has right of appeal to the AAB against the Commissioner's enforcement notice (**section 50(7)**)



55

# Consequences of Breach



- **Criminal investigation and prosecution**
  - **Contravention of a DPP is not an offence per se**
  - **Contravention of a requirement under PDPO other than a DPP is an offence (section 64A)**
  - **Appropriate cases of criminal offences are referred to the Police for criminal investigation and prosecution by Department of Justice**
  - **Liability of key officers – the offences that were committed with the consent or connivance of a director or other officer concerned**  
(section 101E, Criminal Procedure Ordinance (Cap. 221))

# Consequences of Breach

- **Liability of employers and principals under section 65**

- **Would an employee be liable?**

- ✓ *Section 65(1) of the Ordinance*
- ✓ *Act done or practice engaged in by a person*
- ✓ *In the course of his employment*
- ✓ *Be treated as done or engaged in by his employer as well as by him*
- ✓ *Even without employer's knowledge or approval*

- **Would an agent be liable?**

- ✓ *Section 65(2) of the Ordinance*
- ✓ *Act done or practice engaged in by a person as an agent*
- ✓ *With the authority of another person (on behalf of the principal)*
- ✓ *Be treated as done or engaged in by that other person (the principal) as well as by him*
- ✓ *Banks are accountable for the acts done by their agents and contractors (e.g. debt collection agent, marketing agent, IT contractor, waste disposal company etc.)*

57

# Consequences of Breach

- Civil remedy under **section 66**: an individual who suffers damage, including injury to feelings, by reason of a contravention of **PDPO** in relation to his or her personal data, is entitled to compensation from the data user concerned
  - proceedings be brought in the District Court
  - legal assistance for aggrieved persons



58

# Transfer of personal data outside Hong Kong

- S. 33 of the PDPO **prohibits** transfer of personal data outside HK **unless** under **6** specified circumstances (section 33(2)(a)-(f))
- Legislative Intent: personal data transferred outside HK is afforded with **same protection**
- S. 33 **not** yet operative. The Government has engaged a consultant to conduct a **Business Impact Assessment** study (outcome not yet announced). No firm date for implementation
- PCPD's work: the White List (confidential) in response to 1<sup>st</sup> exception and the Guidance (issued in Dec 2014)

# Meaning of Transfer



**Section 33 covers 2 situations:**

**transfer from Hong Kong  
to a place  
outside Hong Kong**

**transfer between 2  
other places  
where the transfer is  
controlled by a data  
user in Hong Kong**



# Meaning of Transfer

“Transfer” is not defined under the PDPO

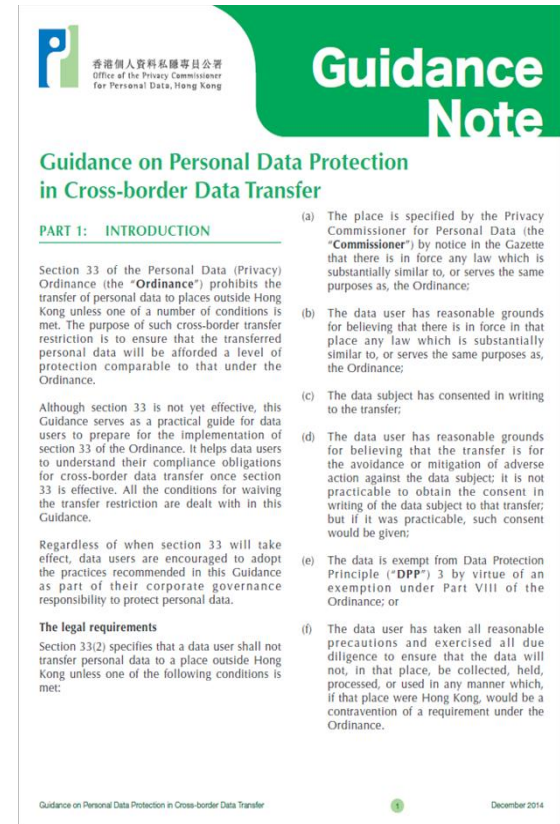
ordinary meaning applies: transmission from one place or person to another (≠ mere transit)

e.g. sending paper or electronic documents containing personal data by courier, post, or electronic means

sending an email to a Hong Kong recipient during which process the data is transmitted via a server/ equipment situated outside Hong Kong because of Internet routing ≠ transfer

# Guidance on Personal Data Protection in Cross-border Data Transfer

- Guidance Note (see website);
- make early preparation;
- understand compliance obligations;
- voluntary compliance as part of corporate governance responsibility to protect personal data



## Exceptions: s.33(2)(a) – (e)

Data user shall not transfer personal data outside Hong Kong unless one of the conditions are met:-

- s.33(2)(a) : Fall within one of the White List jurisdictions (the law in that place is “*substantially similar to or serves the same purposes as*” the PDPO) [Note: The White List is to be kept confidential currently]
- s.33(2)(b) : Data user’s own assessment (the law in that place is “*substantially similar to or serves the same purposes as*” the PDPO)
- s.33(2)(c) : Data subject’s written consent to the transfer
- s.33(2)(d) : Avoidance or mitigation of adverse action against the data subject
- s.33(2)(e) : Exemptions under Part VIII of the PDPO

63

## Exceptions: s.33(2)(f)

**s.33(2)(f) : Data user has taken all reasonable precautions and exercised all due diligence such that personal data transferred will not be handled in a manner that contravenes the PDPO (“Due Diligence Requirement”)**

- **Through either:**

Contractual means; or

Non-contractual means.

# Exceptions: s.33(2)(f) – Contractual means-

An enforceable contract between the parties to the transfer to ensure that the personal data is given equivalent protection

➤ Recommended Model Clauses (“RMC”) (see Schedule to the Guidance)

A set of RMC to assist data users to develop an enforceable contract to satisfy the Due Diligence Requirement

Does not require strict adoption by parties in cross-border transfer (greater flexibility) (vs standard model contract)

Can be a separate data transfer agreement or incorporated into a wider outsourcing agreement

65

# Exceptions: s.33(2)(f) – Contractual means-

- ✓ **Terms can be modified or adapted to suit business needs**
  - **Section I - Core Clauses**
  - **Section II – Additional Clauses**
  
- ✓ **Deals with:-**
  - **Transferor’s obligation**
  - **DPPs to be observed by transferee;**
  - **Parties’ rights in the event of breach;**
  - **Audit requirement;**
  - **Sub-transfer;**
  - **Liabilities; and**
  - **Termination**

**(explanatory notes)**



# Exceptions: s.33(2)(f) – Non-contractual means-

Transferor may adopt the following measures (non-exhaustive):

- Transferor has the right to conduct regular audit and inspection
- Transferor to ensure the transferee has:
  - Sufficient technical competence and organisational measures on data protection with good track record
  - Robust data protection policies and procedures (e.g. data not kept longer than is necessary, data subjects' rights to access and correct their personal data, adequate staff training, etc.)
  - For transfer within intra-group organisations, internal safeguards and policies to reflect the requirements of the PDPO

# Contravention

Offence under s.64A (max fine HK\$10,000)

PCPD may issue enforcement notice for any contravention of s.33 (s.50)

Contravention of enforcement notice is an offence which carries a fine and imprisonment (a daily fine, if continuing offence) (s.50A)

Damage to reputation; loss of customers' trust



# Tips for Cross Border Data Transfer

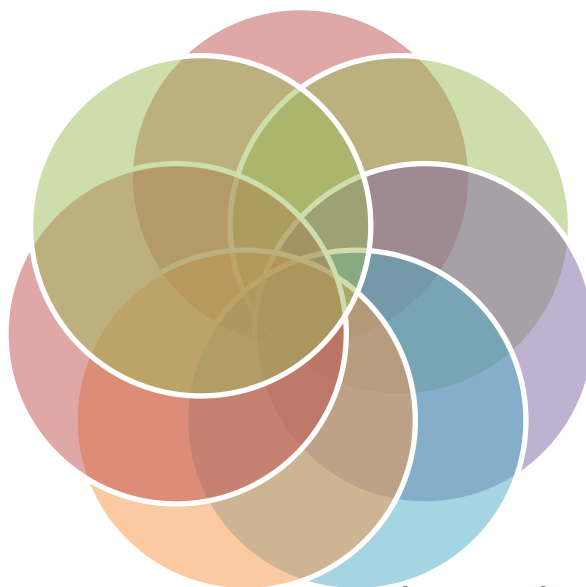
Review existing data transfer strategy

Conduct regular audit and inspection

Control unintended or unnecessary cross-border data transfer

Be transparent about cross border transfer

Check the White List (when it comes into effect)



Keep inventory of personal data (monitor transferee' data handling policies/ whereabouts of personal data)

May adopt multiple measures (e.g. even if the jurisdiction falls within the White List, the parties may still enter into a data transfer agreement) to give more protection

# PCPD's website (PCPD.org.hk)

- PCPD strives to strengthen information on the website, building an important channel to communicate with the public



спасибо  
 danke 謝謝  
 ngiyabonga  
 teşekkür ederim  
 tapadh leat  
 dank je  
 gracias  
 mochchakkeram  
 bedankt  
 hvala  
 maururu  
 thank you  
 go raibh maith agat  
 dziekuje  
 sagolun  
 sukriya  
 kop khun krap  
 arigato  
 takk  
 dakujem  
 merси  
 obrigado  
 terima kasih  
 감사합니다  
 grazie  
 ευχαριστώ  
 merci

PCPD



HK

20



PCPD.org.hk

est.1996

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