University Privacy Campaign 2015/16

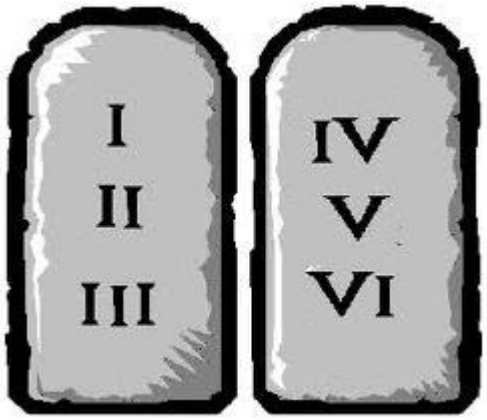
Data Protection in IT Management

Henry Chang
FBCS, CITP, CEng, MIET, CISSP, CISM, CIPT, CIPM
Chief Personal Data Officer
Jan 2016

Note: The contents herein are for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance ("the Ordinance"). For a complete and definitive statement of law, direct reference should be made to the Ordinance itself. The Privacy Commissioner for Personal Data ("the Commissioner") makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the above information. The contents herein will not affect the exercise of the functions and power conferred to the Commissioner under the Ordinance.

Agenda

1. Data Protection Principles
2. The CIA Principles
3. The Privacy by Design Approach
4. Direct marketing requirements
5. Common privacy issues when managing IT systems
6. Use of the latest ICT



The Six Data Protection Principles

Personal Data Definition

Any data:

1. **relating directly or indirectly to a living individual;**

2. **from which it is practicable for the identity of the individual to be directly or indirectly ascertained ; and**

3. **in a form in which access to or processing of the data is practicable.**

Personal Data Examples

	Rumours in social network	Visual checking HKID at registration	Student number	Security CCTV footage
relating directly or indirectly to a living individual	✗	✓	✓	✓
from which it is practicable for the identity of the individual to be directly or indirectly ascertained	✓	✓	✓	✓
in a form in which access to or processing of the data is practicable	✓	✗	✓	✓

Personal Data Definition

Are these personal data?

a) Email addresses
b) IP addresses
c) cookies

Data Protection Principles

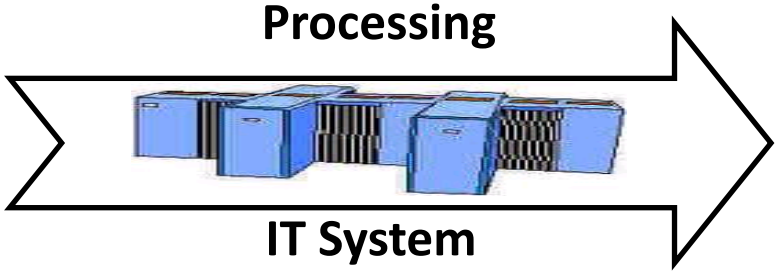
1. Informed Consent
2. Protection
3. Transparency

Data Flow and Data Protection Principles (DPPs)

Personal Data Flow

Collection

Storage, Use or Processing



IT System

Retention / Erasure

DPP 1 – Collection

DPP 3 – Use

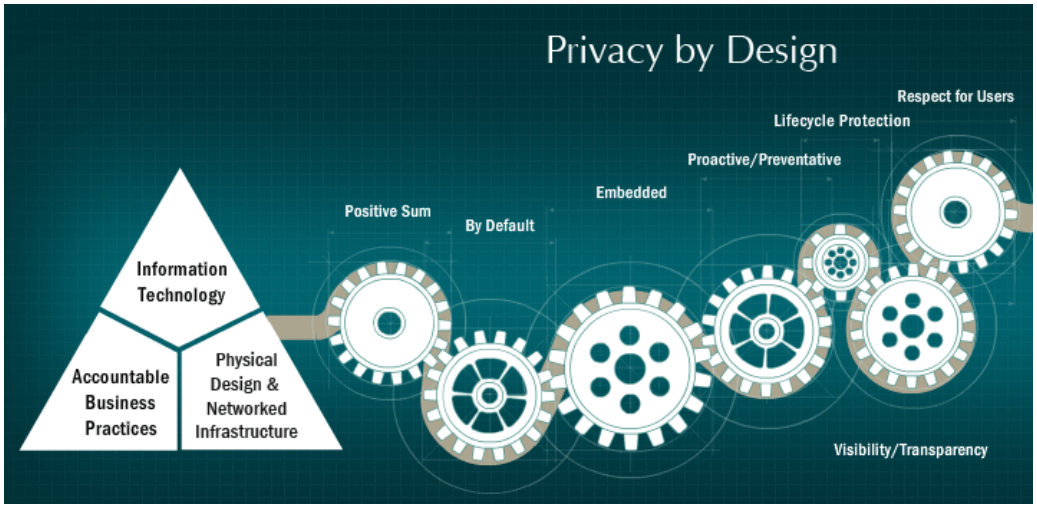
DPP 2 – Accuracy and retention

DPP 4 – Security (IT and physical)

DPP 5 – Transparency

DPP 6 – Rights of access and correction

Privacy by Design



Privacy by Design

Privacy by Design* is the philosophy of embedding privacy from the outset into the design specifications of accountable business processes, physical spaces, infrastructure and information technologies

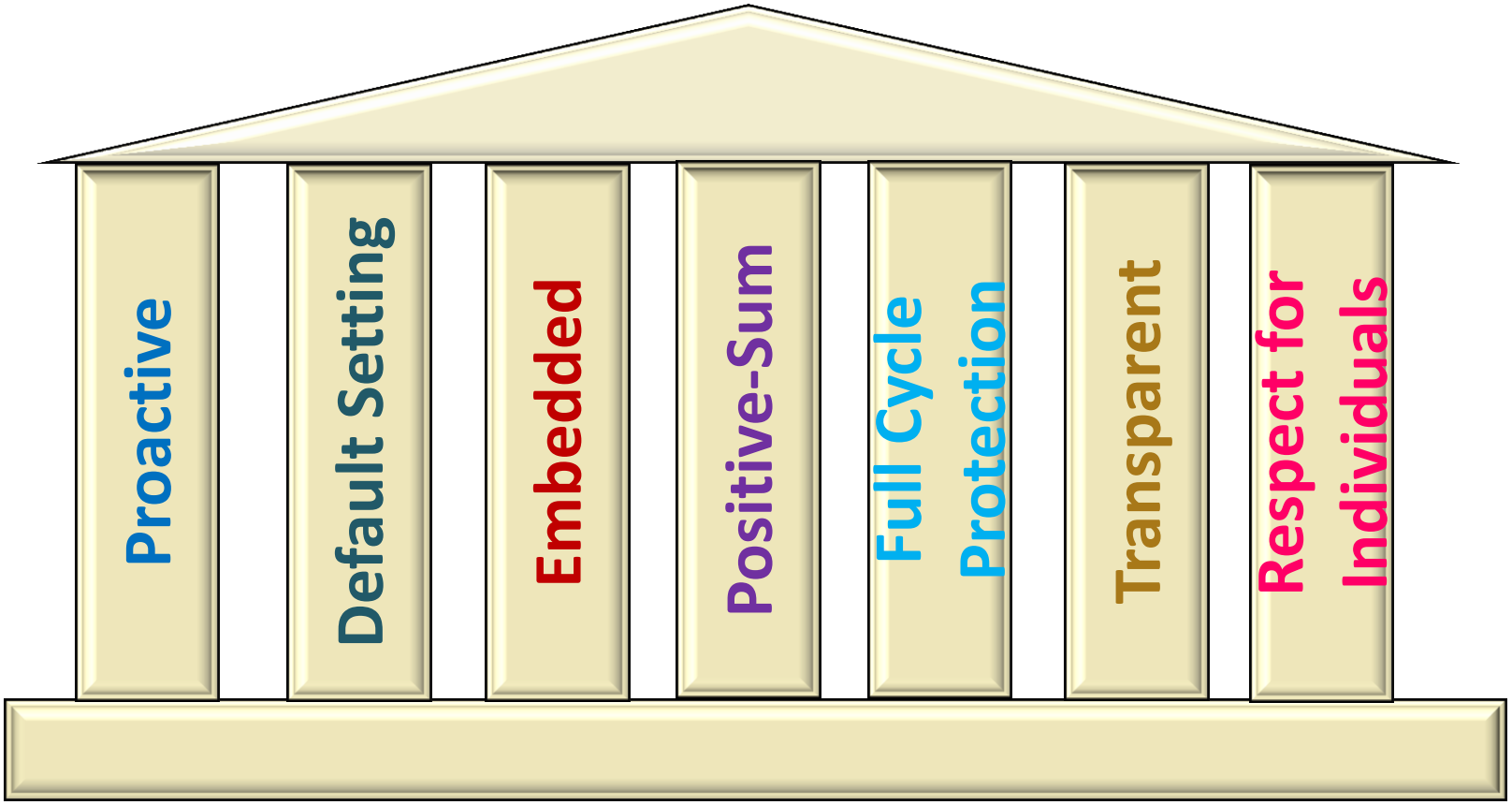
*http://privacybydesign.ca/

The essence of Privacy by Design

A clever person solves problem,

a wise person avoids it.

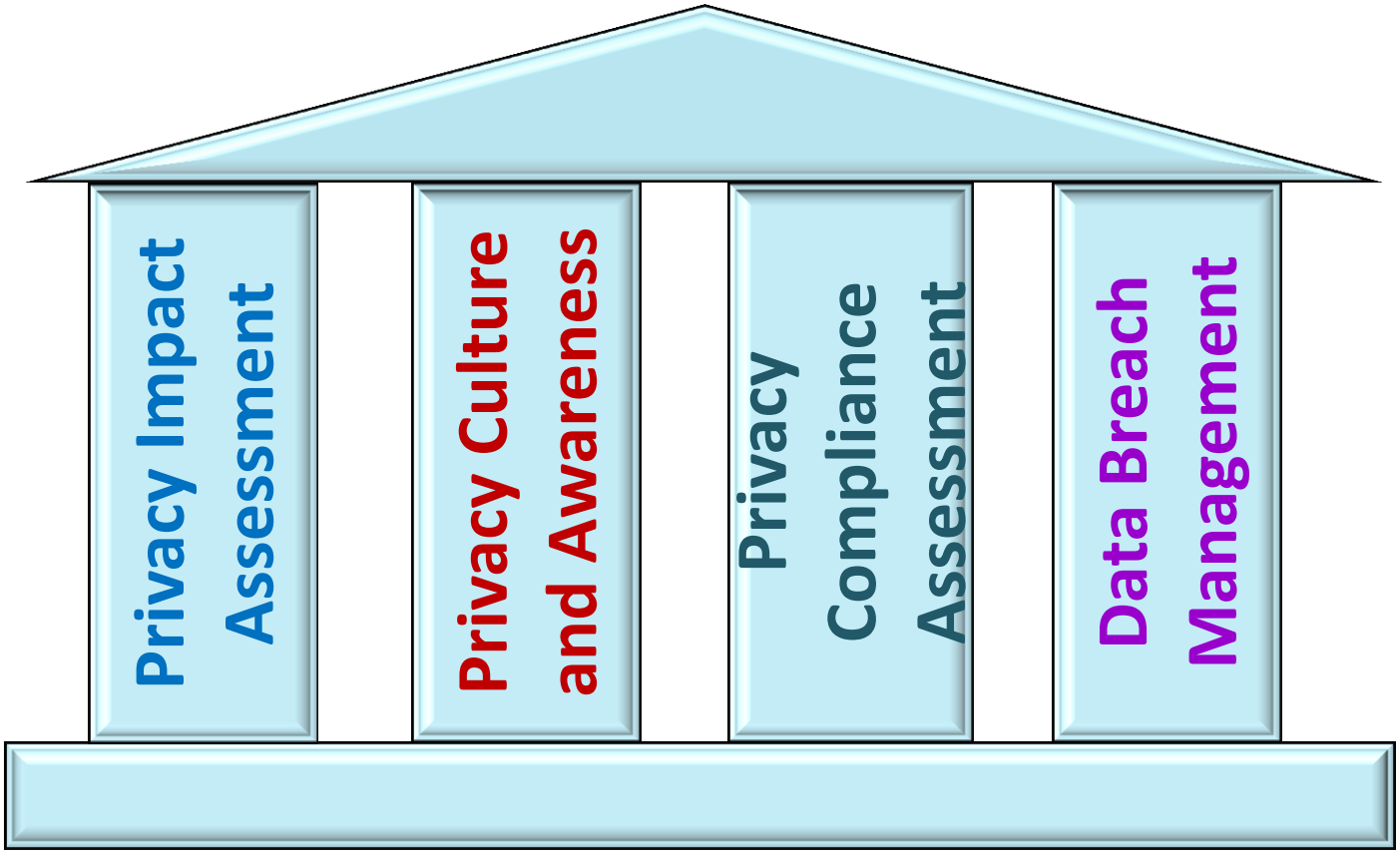
Privacy by Design Principles



Privacy by Design Principles

1. Personal data protection should be proactive (not reactive) and preventive (not remedial) in nature;
2. Personal data privacy should be as the default setting;
3. Personal data privacy should be embedded into the design and not a bolt-on;
4. Personal data privacy design should be "win-win" and not a trade-off against functionality or security;
5. Personal data protection should cover the entire cycle of personal data flow from collection to erasure;
6. Personal data privacy design should be transparent to all stakeholders to allow for verification;
7. Personal data privacy design should be people-centric to address their concerns.

Privacy by Design Tools



Privacy by Design Tools

Privacy Impact Assessment

- A systematic evaluation of a proposal in its impact on personal data privacy with a view to avoiding or minimising adverse impacts.

Privacy Culture and Awareness

- Personal data privacy protection is not a silo compliance issue but a corporate culture that could differentiate an organisation.

Privacy Compliance Assessment

- A systematic assessment on the level of privacy compliance with the Ordinance and any established policies, guidelines and procedures.

Data Breach Management

- Data breach incidents need to be managed proactively and in a planned manner like DRP/BCP.

Direct marketing provisions

Direct Marketing and Sections 35A – 35M

Part VI A: Use of personal data in direct marketing and provision of personal data for use in direct marketing

- **Data subjects to be informed of the direct marketing intention and details; and**

- **consent (or 'no indication of objection') must be obtained from data subjects before direct marketing is to take place; or**
- **written consent (or 'no indication of objection') must be obtained from data subjects before personal data is to be transferred to others for direct marketing.**

- **if the data subject so requests, cease to so use those data without charge to the data subject.**

Direct Marketing and Sections 35A – 35M

Part VI A: Exemptions (35B):

This Division does not apply in relation to the offering, or advertising of the availability, of -

a) social services run, subvented or subsidized by the Social Welfare Department;

b) health care services provided by the Hospital Authority or Department of Health; or

c) any other social or health care services which, if not provided, would be likely to cause serious harm to the physical or mental health of -

   i. the individual to whom the services are intended to be provided; or

   ii. any other individual.

Common privacy issues when managing IT systems

Over-collection or don't care?

Media Statements

Date: 15 December 2014

縱橫遊 www.wwpkg.com.hk

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

(15 December 2014) The Office of the Privacy Commissioner for Personal Data ("PCPD") published an investigation report today 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.

2. The two companies have contravened the Data Protection Principle ("DPP") 1 in Schedule 1 to the Personal Data (Privacy) Ordinance ("Ordinance").

Till death us do part?

Media Statements

恒生銀行
HANG SENG BANK

Date: 15 December 2011

Privacy Commissioner Publishes Three Investigation Reports On Banks' Personal Data Practices

1. The Privacy Commissioner for Personal Data ("the Commissioner") Mr. Allan Chiang published today (15 December) (i) three investigation reports on the personal data practices of two banks and (ii) results of a check against 19 retail banks on their collection of two specific personal data items from savings account applicants.

Investigation results on Hang Seng Bank's prolonged retention of bankruptcy data

9. During the course of a self-initiated investigation prompted by a complaint, it was revealed that Hang Seng Bank had been engaged in the practice of retaining its customers' bankruptcy data for 99 years, without justifiable reasons.

10. The Commissioner is of the view that bankruptcy data should not be kept any longer than 8 years for the reason that a bankrupt will normally be discharged upon expiry of a period between 4 to 8 years beginning with the commencement of the bankruptcy. As such, he found Hang Seng Bank's retention of the bankruptcy data was longer than necessary, thus contravening section 26(1) and DPP2(2) of the Ordinance. The bank has since revised its policy not to retain customers' bankruptcy data for more than 8 years from the respective dates of the declaration of bankruptcy.

Use of social media

參考編號.:2012C03

強積金計劃成員投訴強積金中介人在Whatsapp披露其個人資料

<u>投訴內容</u>

1. 案情摘要

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。

2. 該金融公司的申述

在私隱專員進行調查的過程中，該公司確認他們就該登記時收集了投訴人的姓名及流動電話號碼，但卻沒有收集她的英文名，而該名字是投訴人於Whatsapp 自行設定的用戶名稱。該公司解釋，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。

Contractor's problem or yours?

Media Statements

Date: 15 December 2014

HKA HOLIDAYS
香港航空旅遊

Personal Data Leaked through Inadvertent Use of Mobile Application "TravelBud" by HKA Holidays

(15 December 2014) The Office of the Privacy Commissioner for Personal Data ("PCPD") published an investigation report today concerning 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 the Personal Data (Privacy) Ordinance (the "Ordinance").

Segregation of testing environment

Media Statements

獨立監察警方處理投訴委員會
Independent Police Complaints Council

Date: 26 October 2006

Privacy Commissioner releases the IPCC investigation report

The Privacy Commissioner for Personal Data (the Commissioner) Mr. Roderick B. Woo published today a report (the Report) on the result of an investigation of the leakage on the Internet of personal data relating to complaints made against the Police by the public.

Background

The incident was first reported in a local newspaper on 10 March 2006. Personal data of about 20,000 people who had made complaints to the Police held by the Independent Police Complaints Council (IPCC) were posted on the Internet and became accessible by the public. The Commissioner immediately carried out a self-initiated investigation on 15 March 2006. After commencement of the investigation, the Commissioner received a total of 55 complaints made against the IPCC. The investigation was carried out by way of visits to the IPCC office, visits to the Complaints Against Police Office, interviews of the persons concerned and the taking of statements, examination of documentary records and written representations from the relevant parties as well as oral examination of persons summoned under section 44 of the Personal Data (Privacy) Ordinance (the Ordinance).

Other common issues when managing IT systems

- Weak access and password control
- Lack of administrative control over encryption
- Technical safeguards – three-tier, vulnerability test (don't forget app scanning), privacy-enhancing technologies
- No 'predicable' URLs for information that should be protected by access control
- No 'hidden'/unprotected file in webserver – if it is there, search engines will find it!
- No HKID as password/shared secret!!
- Maintenance files left on webservers
- Check with Google hack!
- SQL injection!!

Cloud Computing

Are you being overshadowed?

Cloud Computing

Or are you on top of it?

Personal Data Protection in the Cloud

Bottom lines of engaging clouds

- Data users are responsible for the protection of personal data

- Outsourcing data processing does not mean outsourcing legal liability

Personal Data Protection in the Cloud

Cloud Characteristics of Particular Concern

- ❑ Rapid transborder data flow

- ❑ Rapid/Loose outsourcing arrangement

- ❑ Standardised contract

Personal Data Protection in the Cloud

Cloud is just a form of outsourcing, so…

- Can the cloud provider unilaterally change the agreement?
- Agreement must allow data users to discharge their duties (such as data access and correction requests), particularly in the case of SaaS
- "Use limitation" to be added to the agreement
- Possible to use end-to-end encryption to protect personal data?

Personal Data Protection in the Cloud

Bottom lines

- Data users are responsible for the protection of personal data
- Outsourcing data processing does not mean outsourcing legal liability
- The amendments to DPP2 and DPP4 on ensuring data processors do not hold on to personal data longer than necessary and exercise reasonable practicable protection

Personal Data Protection in the Cloud

ISO 27018 Code of practice for protection of PII in public clouds acting as PII processors

- Elaboration on ISO 27002 controls
- Specific ISO 29100 controls

Personal Data Protection in the Cloud

Principle	Example of control
Policy compliance	CSP must always process PII in accordance with the service's stated policies that have been disclosed to customers.
End-users' access rights	CSP must offer tools that help customers comply with their data protection obligations to their own end-users, including allow end-users to access, correct and/or erase PII.
Purpose limitation	CSP cannot use PII for marketing or advertising without express consent of customer. Such consent should not be a condition for receiving the service.
Breach notification	CSP must notify customer of any unauthorised access to personal data or to processing equipment or facilities resulting in loss, disclosure or alteration of personal data.
Data deletion	CSP must have and implement policy for data retention and destruction after termination of a contract.

Personal Data Protection in the Cloud

Principle	Example of control
Geographic location of data	CSP must identify countries where data may be stored, and the names of any sub-processors.
Law enforcement requests	CSP must notify customer of legally binding law enforcement requests to disclose customer data, unless such notification is legally prohibited
Confidentiality	CSP must enter into confidentiality agreement with staff who have access to PII and provide appropriate staff training.
Encryption	CSP must encrypt PII that is transmitted over public data-transmission networks
Independent reviews	CSP must subject their service to independent information security reviews at planned intervals, and offer customers independent evidence that appropriate measures are in place to ensure compliance with CSP's policies and procedures.

Personal Data Protection in the Cloud

ISO 27018 CoP for PII protection in public cloud - the sliver bullet?

- Too new to say
- It is a Best Practice like ISO27002, not a Standard – assessment on actual controls may be required

Privacy by Design – when applying it to app development

1. Is the access of the information necessary?
   a) If access is necessary, has it been explained in the collection statement/privacy policy?
   b) If access is necessary, is the uploading of the information necessary?
   c) If uploading is necessary, is the storage necessary?
   d) If access is necessary, is the sharing/transferal of the information necessary?
2. What other information is being collected/combined/associated?
3. What safeguards (such as validation, proper encryption and access controls) are in place to the information ccessed/transmitted/shared/kept?
4. Is the retention policy reasonable and can app users opt out of any of these collections and erase/delete collected information and accounts?
5. Do you have a set of process and procedures in place to fulfil the data access and correction obligation?

Best Practice Guide for Mobile App Development

Please check out the "Best Practice Guide for Mobile App Development"

http://www.pcpd.org.hk/english/publications/files/Mobileapp_guide_e.pdf

Best Practice Guide for Mobile App Development:

Checklist for self-evaluation

表 2 — 檢查表
TABLE 2 – Checklist

問題 Questions	資料類別 Types of Data										操作 Operations		
	裝置獨特識別碼 Unique device identifier	定位位置 Locations	流動電話號碼 Mobile phone number	聯絡人 / 通訊錄 Contacts list/address book	行事曆 / 提示 Calendar/ reminder	儲存的相片 / 短片 / 錄音 Stored photos/ videos/ recordings	SMS/MMS/ 電郵訊息 SMS/ MMS/email messages	通話記錄 Call logs	瀏覽記錄 Browser history	程式名稱 / 帳戶名稱 App names/ account names	使用麥克風 / 鏡頭 Use microphone/ camera	要求 / 容許用家登入 Require/allow user login	提取其他資料 Obtain other info
1. 是否絕對需要讀取 / 收集 / 使用資料以供程式的運作？見 E1 Is the access/collection/use of the data absolutely necessary for the app's operation? See E1													
2. 會否從流動裝置上載 / 傳輸資料（或衍生資料）？見 E2 Will the data (or derived data) be uploaded/transmitted from the mobile device? See E2													
3. 會否儲存或保留流動裝置的資料（或衍生資料）在別處？見 E3 Will the data (or derived data) be stored or kept elsewhere from the mobile device? See E3													
4. 會否將資料（或衍生資料）與從別處取得的其他個人資料結合 / 串連？見 E4 Will the data (or derived data) be combined/correlated with other data of the individual obtained elsewhere? See E4													
5. 會否在你的業務內分享（例如跨程式整合）或與其他人士 / 機構分享資料（或衍生資料）？見 E5 Will the data (or derived data) be shared within your business (e.g. for cross-app integration) or with other parties? See E5													
6. 會否將資料（或衍生資料）用作建立個人的資料檔案？見 E6 Will the data (or derived data) be used for profiling of individuals? See E6													
7. 會否將資料（或衍生資料）用於直接促銷？見 E7 Will the data (or derived data) be used for direct marketing? See E7													
8. 是否已擬備涵蓋所有資料類別的《收集個人資料聲明》及 / 或《私隱政策聲明》？見 E8 Has a Personal Information Collection Statement and/or Privacy Policy Statement been prepared to cover all data types involved? See E8													
9. 你是否已考慮程式用家在私隱上的期望？見 E9 Have you taken into account app users' privacy expectations? See E9													
10. 你的程式有否使用第三者工具（軟件庫、廣告網絡等）（或你是否這些工具的供應商）？見 E10 Do you use third-party tools (software library, ad networks etc.) in your app (or are you the provider of these tools)? See E10													

Privacy Policy St

The protection of priv
data is the concern o
the Hong Kong Obser
personal data and are
implementing and co
protection principles
the Personal Data (Pr

iOS version

1. The Governme
Administrative
servants and a
will record visit
("the app") with
identifiable infc
general statisti
statistical repo
with, or concer
help improve th
2. To provide loca
the app would
present data th
user by retrievi
of the Hong Ko
User's location
out from the ap
turn on Locatic
service. Please see paragraph 5 below for details.).

Android version

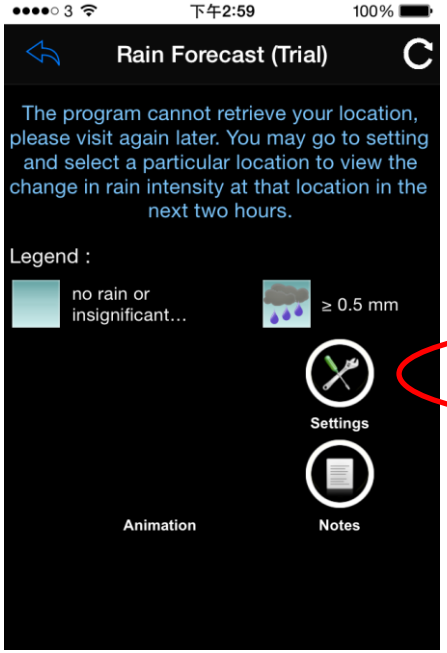
1. The HKO will record visits to the "MyObservatory" ("the app") without collecting any personal identifiable information from users. Such general statistics are collected to compile statistical reports and diagnose problems with, or concerning, computer systems to help improve the app.
2. To provide location-based weather service, the app would get user's location and present data that is most relevant to the user by retrieving information from servers of the HKO. User's locations would not be transmitted out from the app. This feature requires user's authorization on "approximate location (network-based)" and "precise location (GPS and network-based)".
3. To allow user to gain access to HKO's Dial-A-Weather (DAW) service, the app would call the DAW hotline when user presses DAW link in the app. The app would not access to any information in the address book of user's smartphone. This feature requires user's authorization on "directly call phone numbers".
4. To reduce waiting time for downloading data after loading the app with a view to improving user experience, the app would

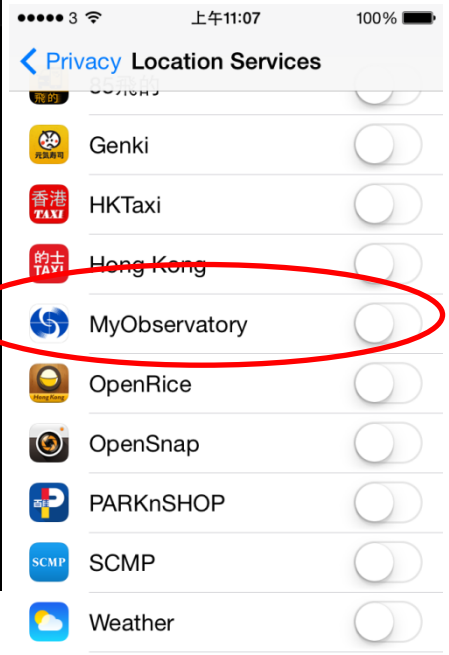
The good - transparent

- Available before installation
- (Nearly) single page and in simple language
- Specific to the types of data accessed
- Assured users what it would not do
- But – don't copy this…

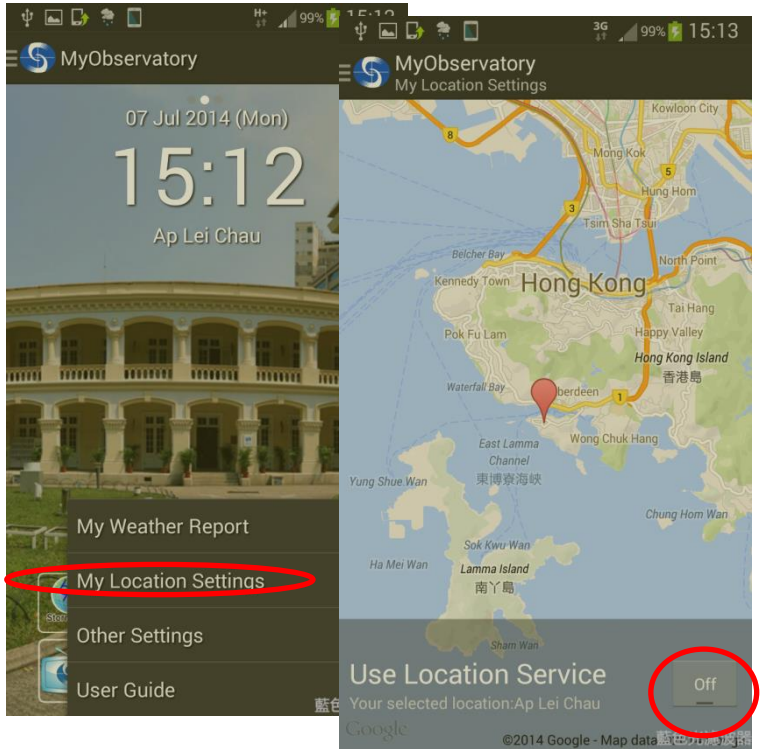
The good - build your own granular controls

For iPhone:





Why not 'port' the logic to Android?



Physical Tracking by devices

- Tracking by smartphones;
- Tracking by goods tagged with RFID;
  - No authentication needed for reading tags;
  - Tags carry standarised Electronic Product Codes

Physical Tracking - risks

- Sense of violation of rights;
- Re-identification of individuals from supposedly anonymous data;
- Profiling and negative impact to individuals without the individual knowing why.

Privacy Impact Assessment

- Minimisation of surprise
- Minimisation of data
- Minimisation of risk

Bring Your Own Device (BYOD)

Aims

- Protection of personal data of customers
- Protection of personal data of BYOD users/owners
- Conflicting demands?

Bring Your Own Device (BYOD)

Bottom-line

- Smartphone has an inherently insecure architecture
- Don’t use vanilla smartphone as BYOD equipment without additional protection

Bring Your Own Device (BYOD)

Solutions

- Protect personal data and app, not the device
- Leave the protection of the device to the hands of the owners

Bring Your Own Device (BYOD)

Scenarios

If data/app are protected from access by other apps
- Harder for malware and accidental disclosure
- Harder for users to backup/syn the data

If apps need to be authenticated separately
- Harder for unauthorised users to access data

If data is encrypted or time-bombed
- Harder for wrongful disclosure due to data breach

List of ICT related publications

www.pcpd.org.hk/Resources Centre/Publications/Guidance Notes/Information and Communications Technology

- Guidance on Collection and Use of Biometric Data
- Guidance on Data Breach Handling and the Giving of Breach Notifications
- Best Practice Guide for Mobile App Development
- Guidance on the Use of Portable Storage Devices
- Guidance for Data Users on the Collection and Use of Personal Data through the Internet
- Guidance on Personal Data Erasure and Anonymisation
- Guidance on CCTV Surveillance and Use of Drones
- Guidance on Use of Personal Data Obtained from the Public Domain
- Guidance on Personal Data Protection in Cross-border Data Transfer

www.pcpd.org.hk/Resources Centre/Publications/Information Leaflets/Information and Communications Technology

- Privacy Impact Assessments
- Cloud Computing
- Privacy Implications for Organisational Use of Social Networks
- Online Behavioural Tracking
- Personal Data Privacy Protection: What Mobile Apps Developers and their Clients should know
- Outsourcing the Processing of Personal Data to Data Processors