



# PolyU IT Security in our Daily Life



## New Development in Personal Data Privacy related to Mobile App

*Henry Chang, IT Advisor*

*Office of the Privacy Commissioner for Personal Data, Hong Kong*

*13 February 2015*



# Personal Data Privacy related to Mobile App



- Background and issues identified
- Data Protection Principles in apps development
- Best Practice on designing privacy-friendly mobile apps



## Disclaimer

The contents herein are for general reference only. It does not provide an exhaustive guide to the application of or the compliance with 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 information here. The contents herein will not affect the exercise of the functions and power conferred to the Commissioner under the Ordinance.



## Issues identified in the past



- Lack of app specific and clear privacy policies
- Excessive collection of data
- Inadequate security measures
- Lack of options/opt-outs for app users



## Issues identified in the past



**Lack of app specific and clear privacy policies**



# 2013 and 2014 Mobile App Surveys



## Top 60 apps that accessed smartphone data

### May 2014

- 55% provided privacy policy
- 15% of the policies that were tailor-made to apps
- 8% app developers had not provided sufficient details to identify themselves
- 6% not easily readable

### May 2013

- 60% provided privacy policy in website only
- 8% of the policies that were tailor-made to apps
- 60% app developers had not provided contact details
- 11% in в другом языке or not easily readable



## Issues identified in the past



## Excessive collection of personal data



# Excessive collection of HKID numbers

## Media Statements

**Date: 15 December 2014**

### **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").





## Issues identified in the past



**Inadequate security protection**



# Inadequate security protection

## Media Statements

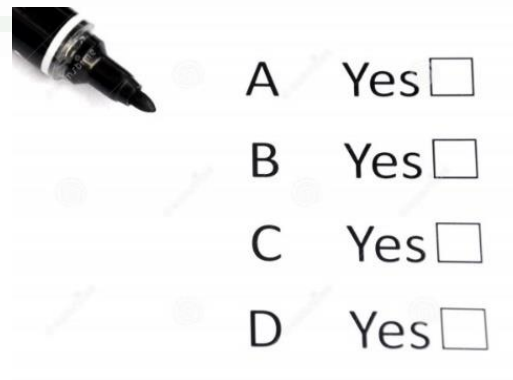
**Date: 15 December 2014**

### **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<sup>1</sup> 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").



## Issues identified in the past

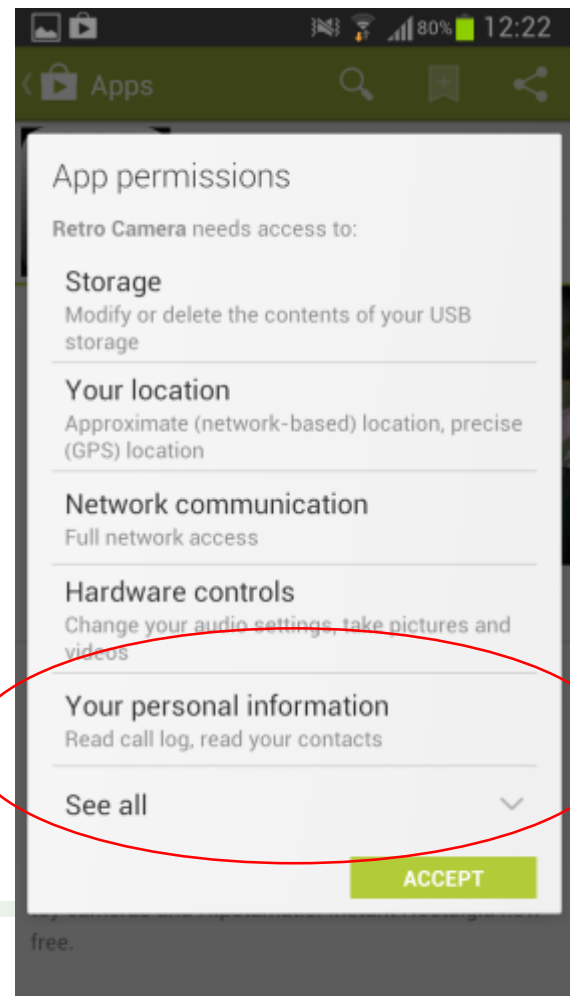
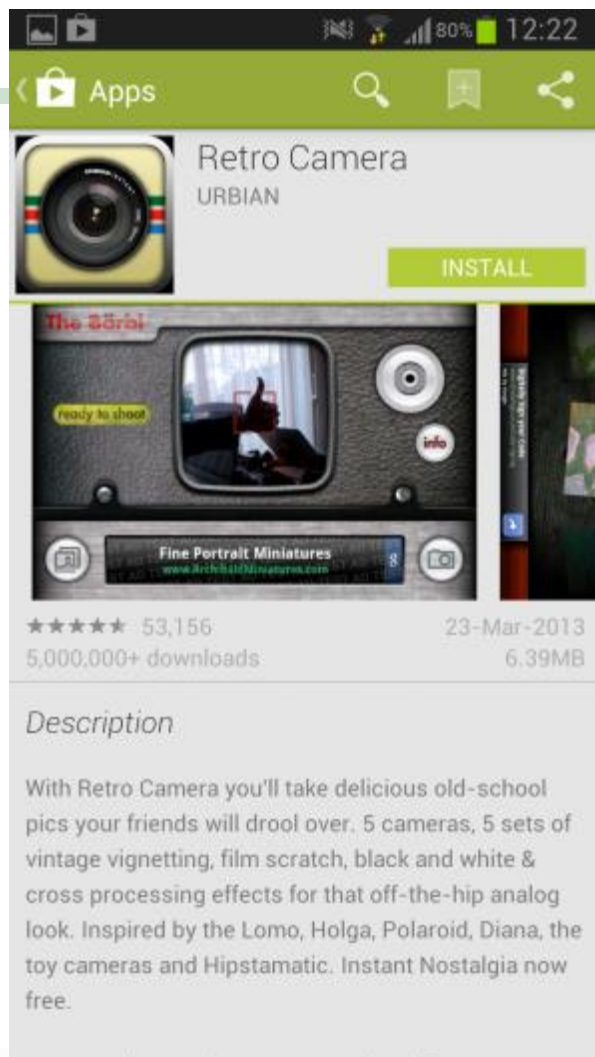


A	Yes	<input type="checkbox"/>
B	Yes	<input type="checkbox"/>
C	Yes	<input type="checkbox"/>
D	Yes	<input type="checkbox"/>

**Lack of options/opt-out**



## Lack of options/opt-out



- It is unclear why access is needed
- Even if access is needed, can app user opt out of this non-core function?



## Personal Data Privacy related to Mobile App

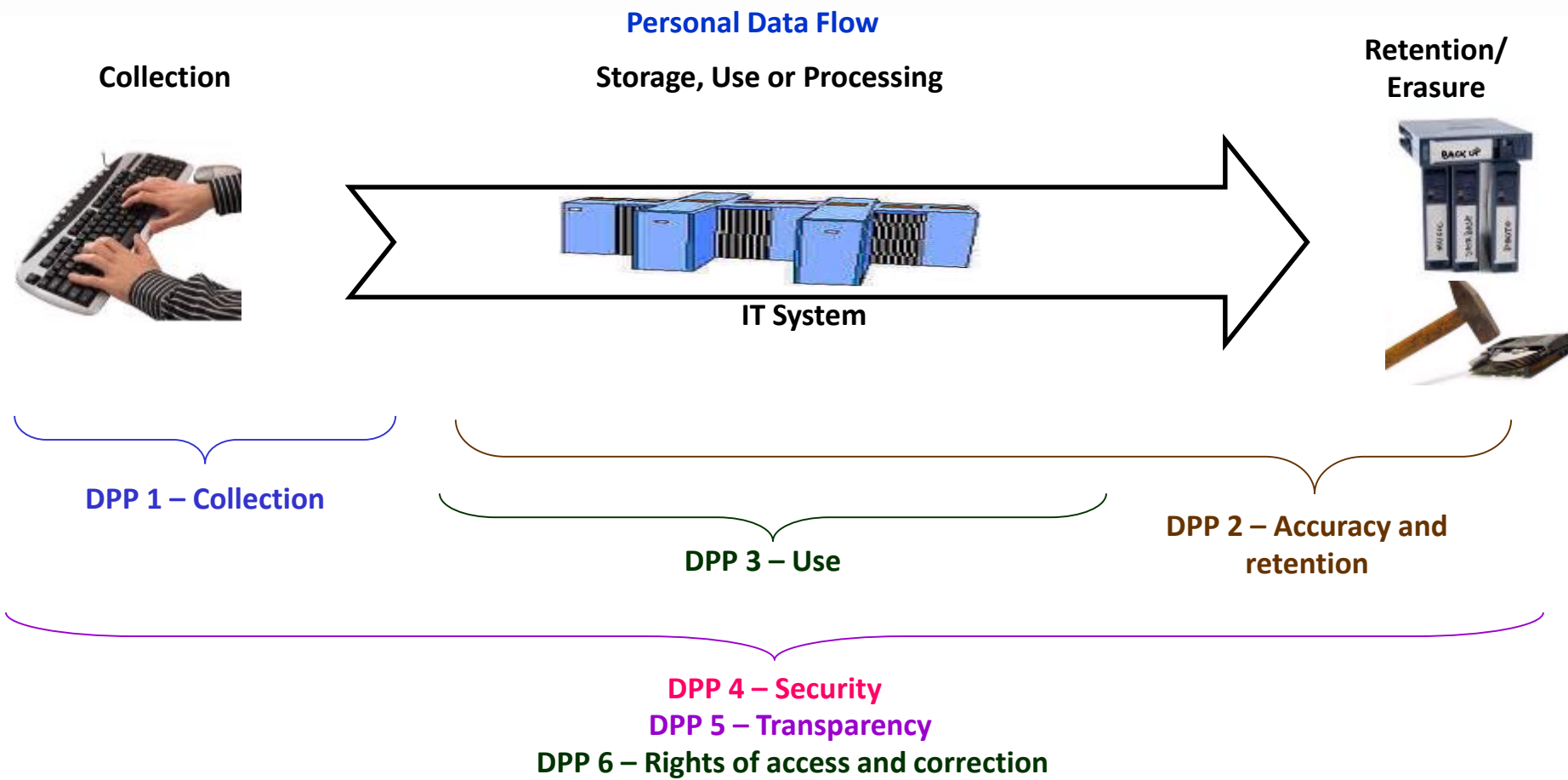


**What are the basic data protection principles?**



# Data Flow and Data Protection Principles (DPPs\*)

\*<http://www.pcpd.org.hk/english/ordinance/ordglance1.html#dataprotect>





# The Six Data Protection Principles



## 1. Purpose and Manner of Collection

- Collection must be directly related to purposes, and is lawful, fair, necessary, adequate and not excessive;
- Inform data subjects of purposes, class of transferees, consequence of not providing the data, and the rights to access and correction;
- Ask yourself if the purpose of collection on each piece of data can be justified.

## 2. Accuracy and Duration of Retention

- Data should only be used if it is considered accurate;
- Data should not be kept longer than necessary (including by contractors);
- Consider the risk or impact if inaccurate data is used, or data is kept longer than is required;
- Have you provided means to data subjects to remove their accounts?

## 3. Use of Personal Data

- Data should only be used for the original purposes unless further consent is obtained;
- Even if you consider the new use is beneficial to app users, if they have not been properly informed, you are changing the use and need to seek their consents.





# The Six Data Protection Principles



## 4. Security of Personal Data

- Appropriate security measures to be applied (including by contractors);
- Have you applied appropriate encryption, hashing or masking during storage and transmission, including the transferal to third parties?
- Assess the adverse impact of any operating system upgrades or features.

## 5. Information to be Generally Available

- Transparency of personal data policies and practices is needed;
- Is the app-specific privacy policy statement readily accessible before app installation?
- Even if you do not think you are collecting personal data, you should consider making it known clearly in a privacy policy statement as smartphone is often considered a very personal device to many.

## 6. Access to Personal Data

- Ensure mechanism is in place to respect the rights of data subjects for access and correction of personal data.





# 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 – when applying it to app development



- Is the access of the information necessary?
  - If access is necessary, is there a clear/accessible privacy policy/notice?
  - If access is necessary, is the uploading of the information necessary?
    - If uploading is necessary, is the storage necessary?
  - If access is necessary, is the sharing/transferral of the information necessary?
- What other information is being collected/combined/associated?
- What safeguards (such as encryption and access controls) are in place to the information accessed/transmitted/shared/kept?
- Can mobile user opt-out of any of these and erase accounts?



## Good Example



**A best-practice example**



#### Android version

### 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 tl

2. To provide loca the app would present data th user by retrievi of the Hong Ko User's location out from the a turn on Locatic service. Please see paragraph 5 below for details.).

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

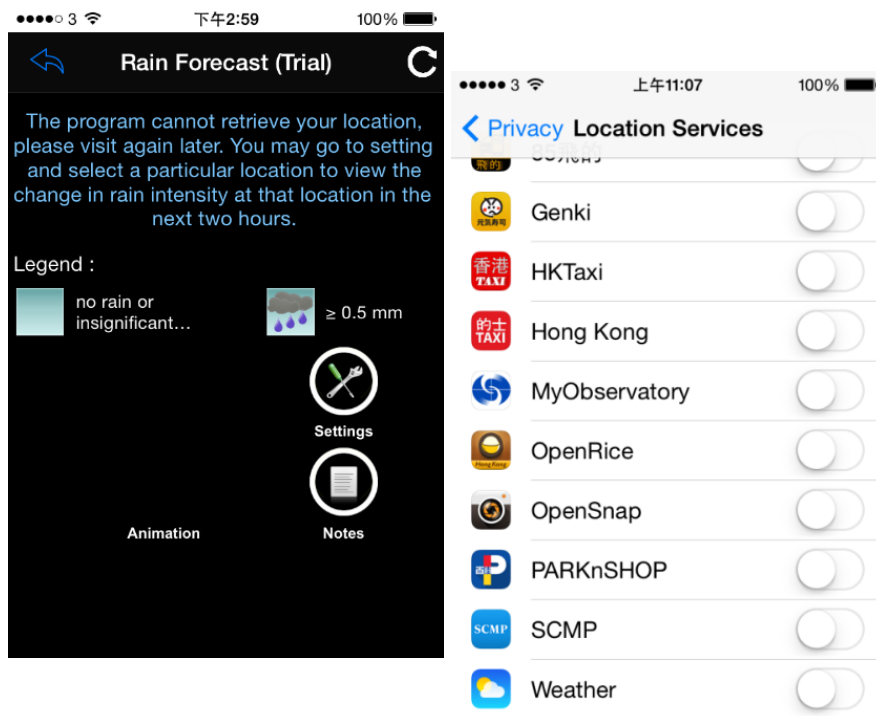
## The good - transparent

- 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...

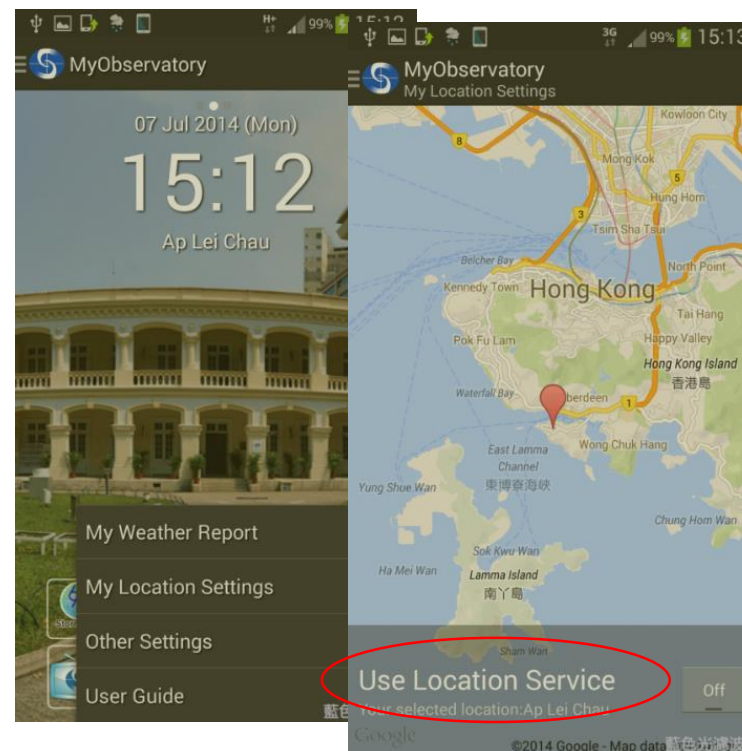


# The good - build your own granular controls

For iPhone:

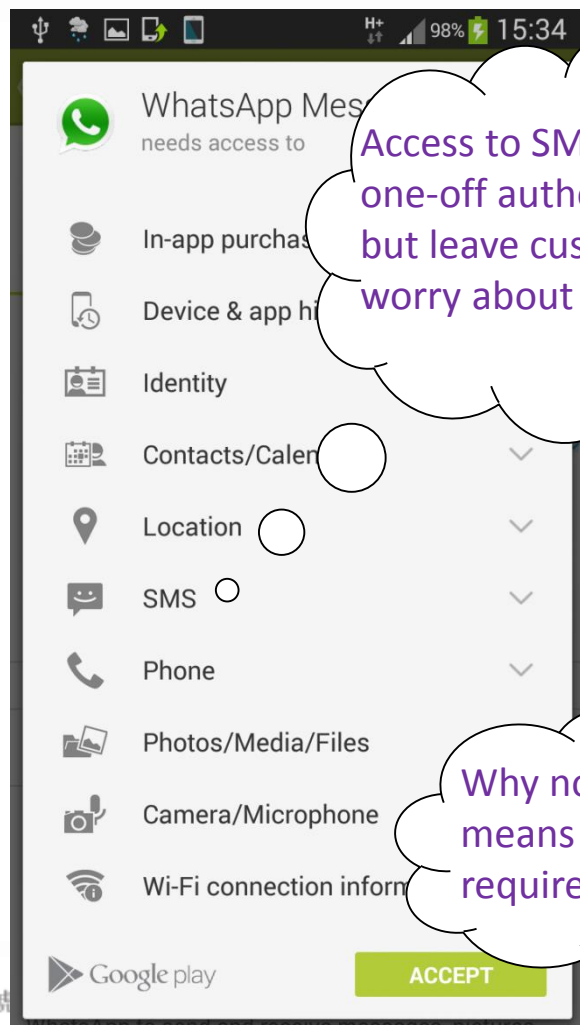


Why not 'port' the logic to Android?



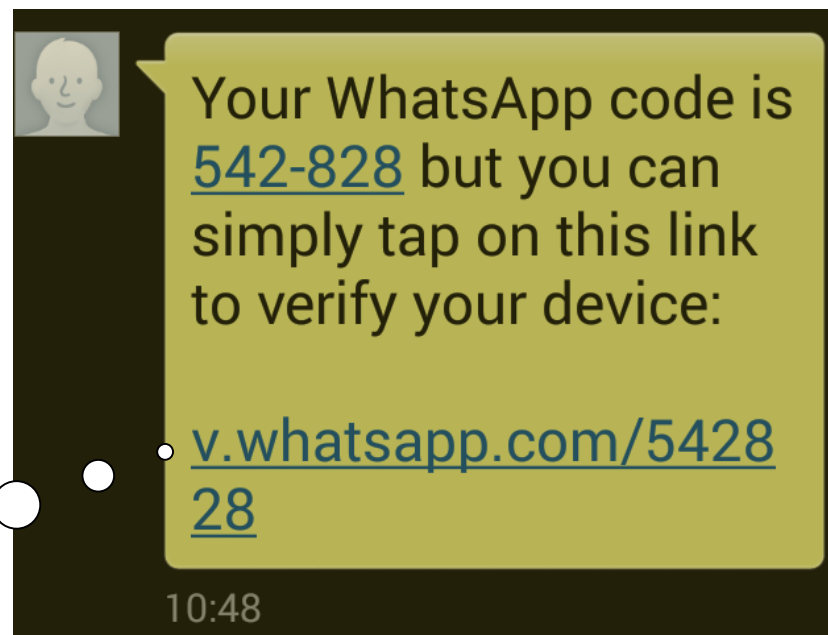


## Do you really need access to SMS just to use it once?



Access to SMS only for a one-off authentication but leave customers to worry about privacy.

Why not use another means that would not require permission?







# Best Practice Guide for Mobile App Development

[http://www.pcpd.org.hk/english/resources\\_centre/publications/guidance/files/Mobileapp\\_guide\\_e.pdf](http://www.pcpd.org.hk/english/resources_centre/publications/guidance/files/Mobileapp_guide_e.pdf)



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

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





# Best Practice Guide for Mobile App Development

## Modular and flow-chart approach

### 何時閱覽

#### WHEN TO READ

你應在開始計劃開發程式時便閱覽本指引。對企業來說，在開始階段便融入保障私隱的概念，相比日後為符規才作出這方面的調整，前者的花費會較少，而其對程式功能的影響也較為輕微。

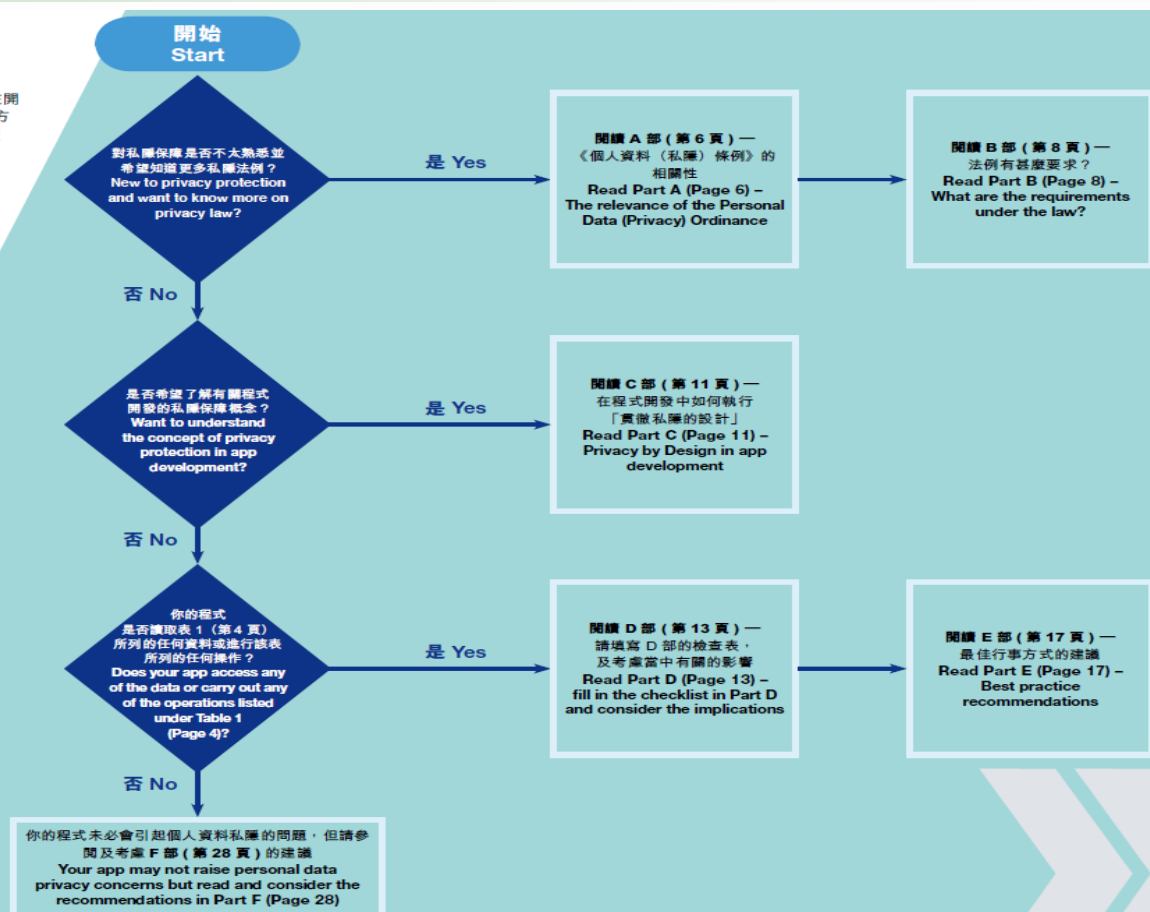
You should read it before you start planning your app development project. Building in privacy protection at the outset will be less costly for the business and will have less impact on your app functions compared with adjustment for compliance at a late stage of the project.

### 如何使用本指引

#### HOW TO USE THIS GUIDE

為方便參閱，本指引由幾部分組成，每一部分均可獨立閱覽。有關本指引的使用，可參考右面的流程表的建議：

This guide comprises a number of parts which may be read independently. The flow chart on the right suggests how this guide may be used.

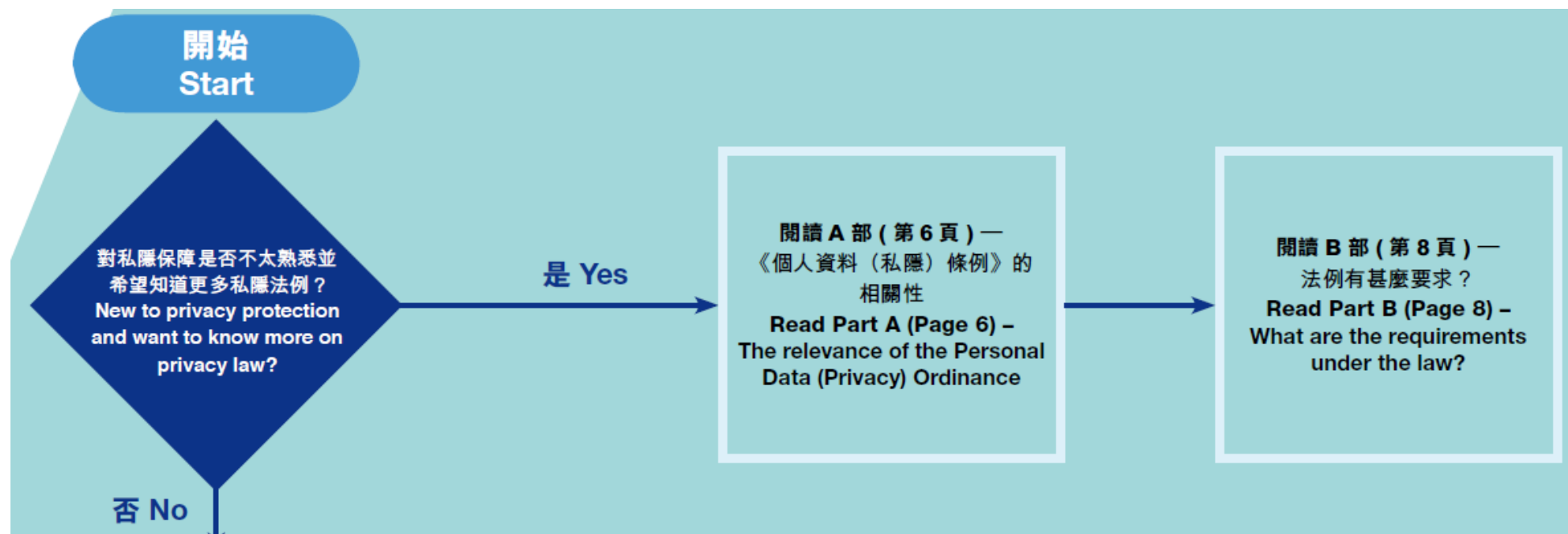


開發流動應用程式最佳行事方式指引  
Best Practice Guide for Mobile App Development



# Best Practice Guide for Mobile App Development

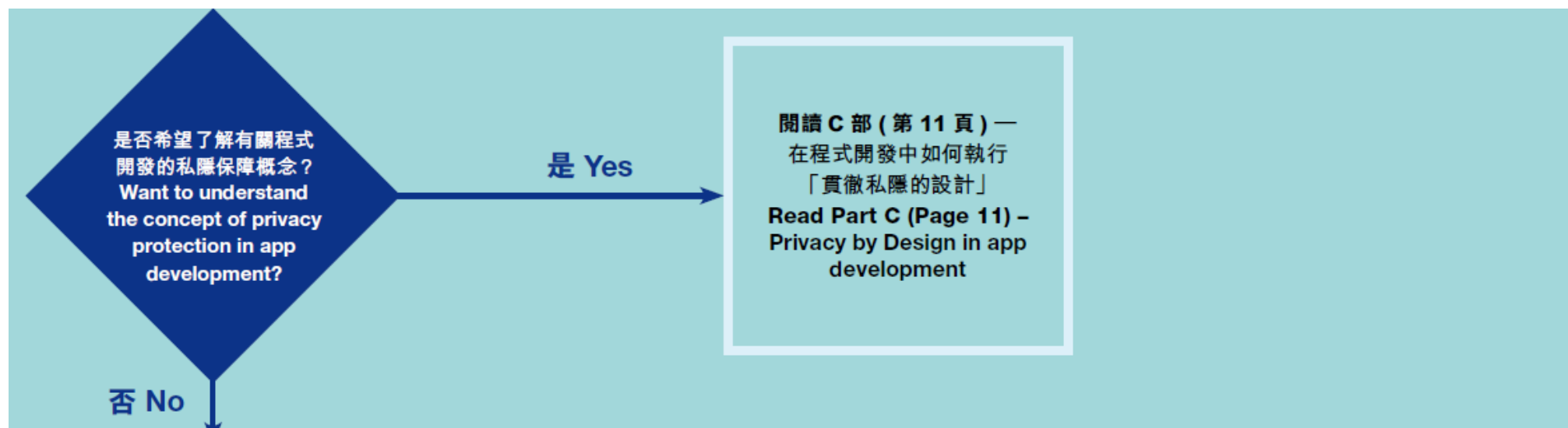
## Legal requirements





# Best Practice Guide for Mobile App Development

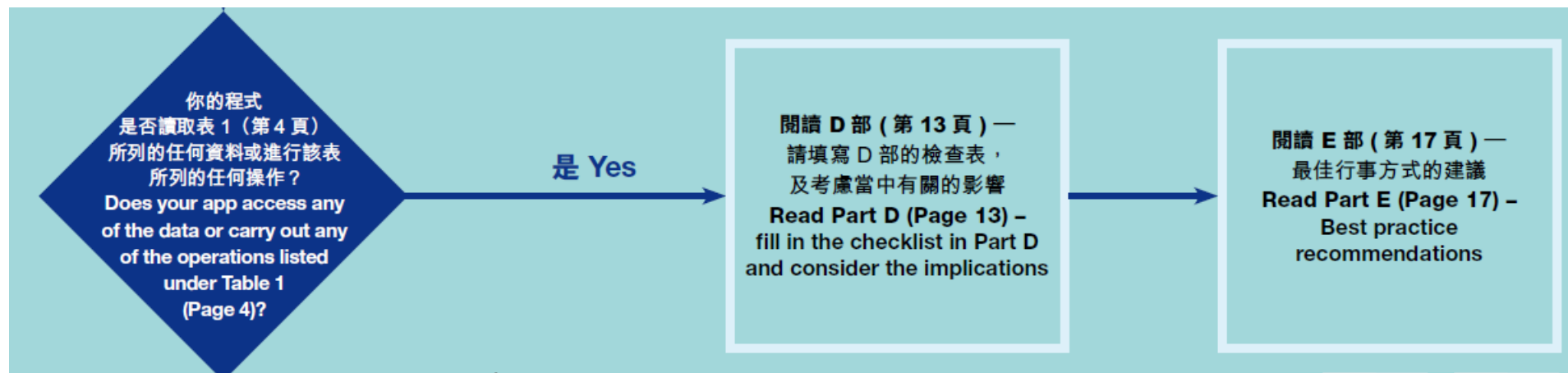
## Privacy by Design explained





# Best Practice Guide for Mobile App Development

## Best practice recommendations





# 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	通話紀錄 Call logs	瀏覽紀錄 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 Require/allow user login	獲取其他資料 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戶在私隱上的期望？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													



# Best Practice Guide for Mobile App Development Transparency





# Your app's name could be here next year...

## Media Statements

**Date: 15 December 2014**

### **Privacy Commissioner Finds Transparency of Privacy Policies Wanting in Local Mobile Applications**

(15 December 2014) The Office of the Privacy Commissioner for Personal Data ("PCPD") conducted a survey<sup>1</sup> of 60 popular mobile applications ("apps") developed by Hong Kong

#### **Privacy-friendly yet Popular Apps, such as the ~~MyObservatory~~, are Viable**

10. Despite the prevalence of disappointing privacy features, PCPD was impressed by the app *MyObservatory*<sup>6</sup> 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.





## Privacy Concern on Mobile App Development

