Mobile App Development Forum on Privacy and Security
The Office of the Privacy Commissioner for Personal Data, Hong Kong
21 April 2016

Privacy by Design and Best Practice Guide on Mobile App Development

Henry Chang, Chief Personal Data Officer
Office of the Privacy Commissioner for Personal Data, Hong Kong

Privacy by Design and Best Practice Guide on Mobile App Development

- **Basic principles of data protection**
- **Case studies on the good and the bad**
- **Best practice guide for mobile app development**

Developing Mobile Apps with Privacy Protection in Mind

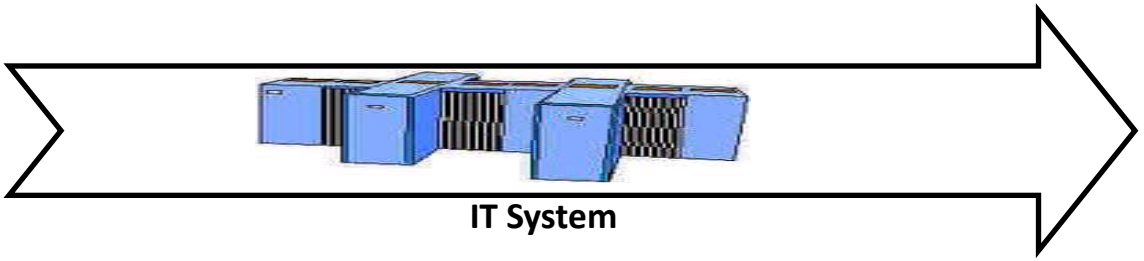
Basic principles of data protection

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

DPP 5 – Transparency

DPP 6 – Rights of access and correction

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.

Data Minimisation!

Privacy by Design – When Applying 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 accessed/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 to fulfil the data access and correction obligation?**

Technical Considerations
(To be covered by PISA and HKCERT)

- **Use reliable software development tools (SDKs; libraries)**
- **Understand what access third-party tools (such as those from Flurry) will have to mobile device data**
- **Use most granular/specific/least privileged calls you can**
- **Remember Confidentiality, Integrity and *Accountability***
- **Be familiar with mobile-specific vulnerabilities/hacking techniques**
- **Perform code-review and software testing**

Case studies on the good and the bad

The good, the bad and the ugly…

Examples

The good…

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

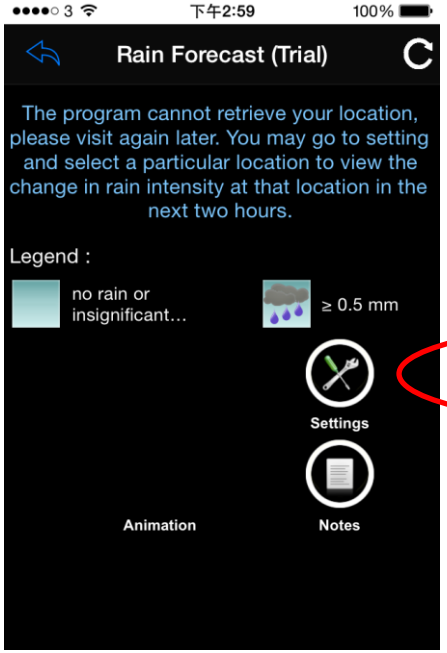
1. The HKO will record visits to the "MyObservatory" ("the app") without collecting any personal identifiable information from users. Such general statistics are collected to compile statistical reports and diagnose problems with, or concerning, computer systems to help improve the app.
2. To provide 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

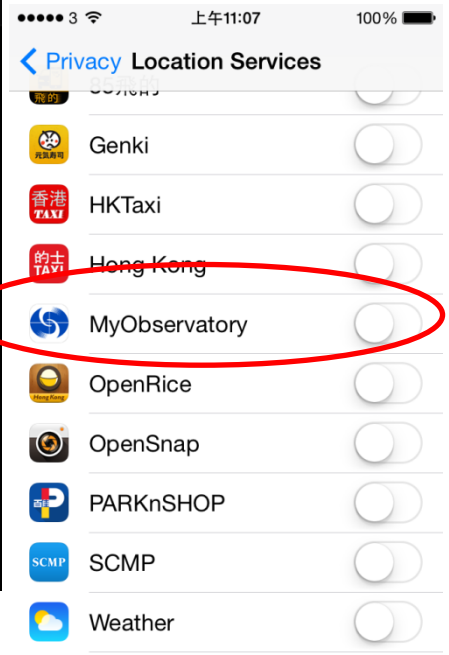
The Good - Transparent

- **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…**

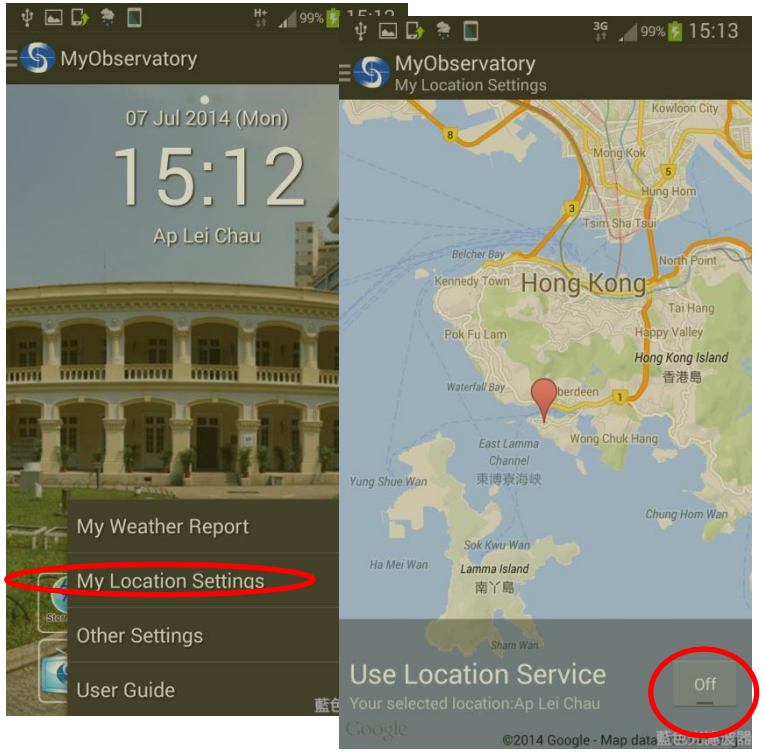
The Good - Build Your Own Granular Controls

For iPhone:





Why not 'port' the logic to Android?



Examples

and the ugly…

Mistake or Don't Care?

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").

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

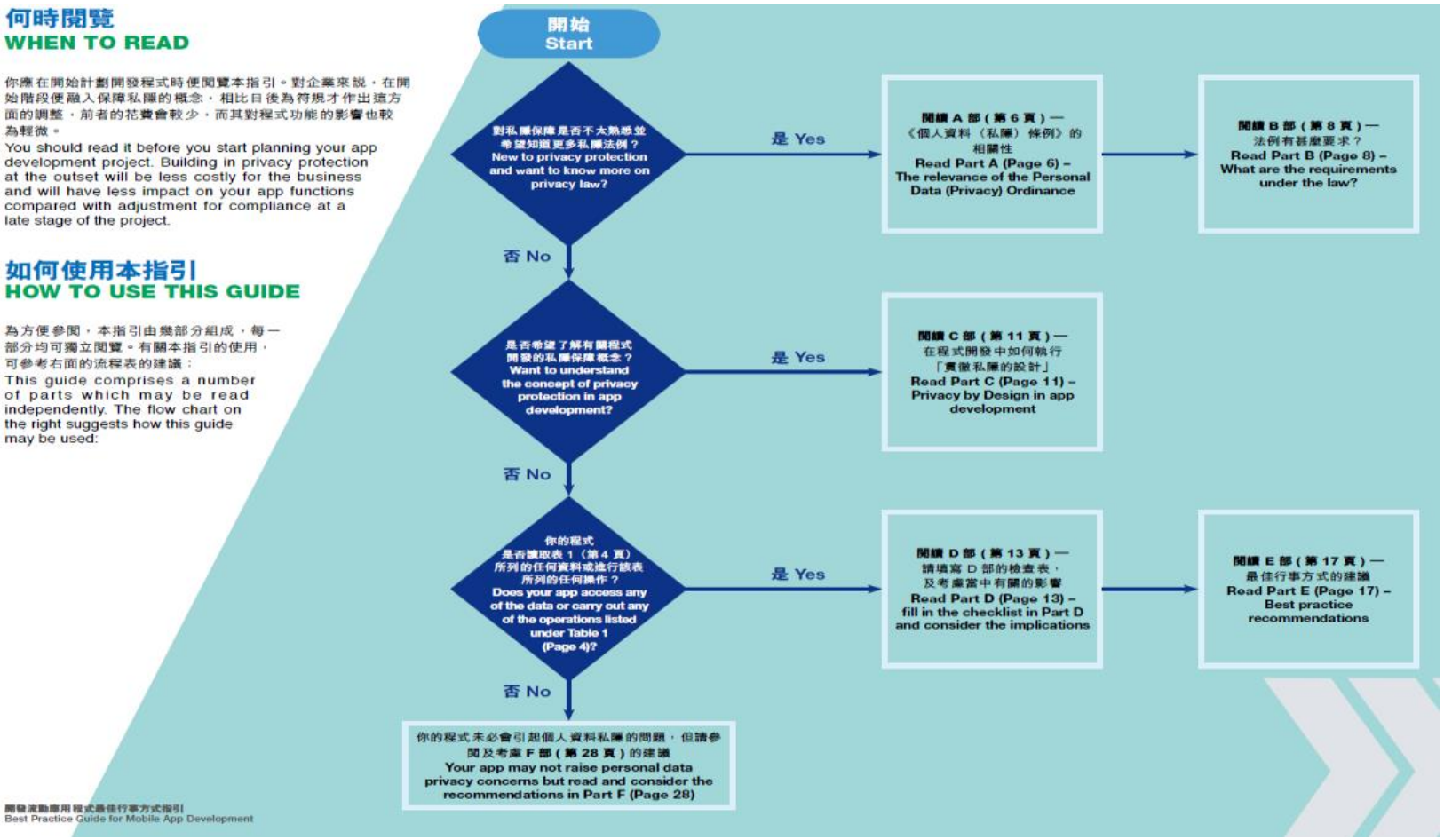
(15 December 2014) The Office of the Privacy Commissioner for Personal Data ("PCPD") published an investigation report today concerning the excessive collection of personal data by Worldwide Package Travel Service Limited ("Worldwide Travel") from customers when they enrolled for the company's loyalty 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").

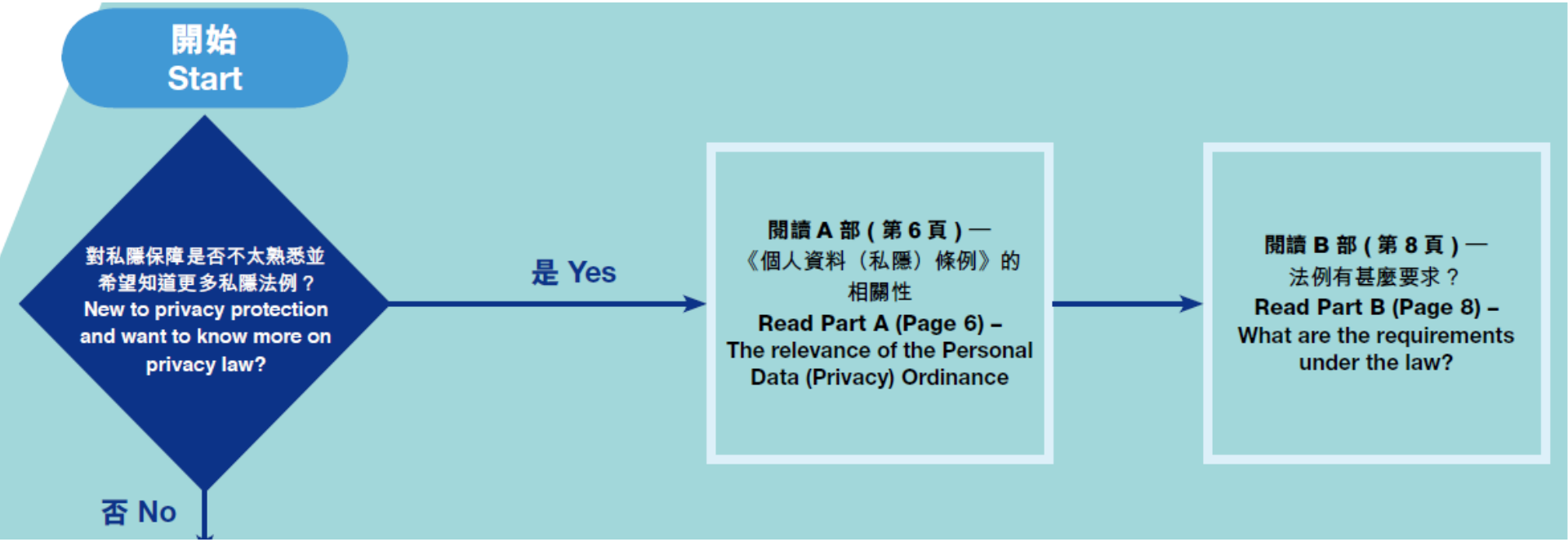
Best Practice Guide for Mobile App Development

PCPD Website -> Resources Centre -> Publications -> Guidance Notes

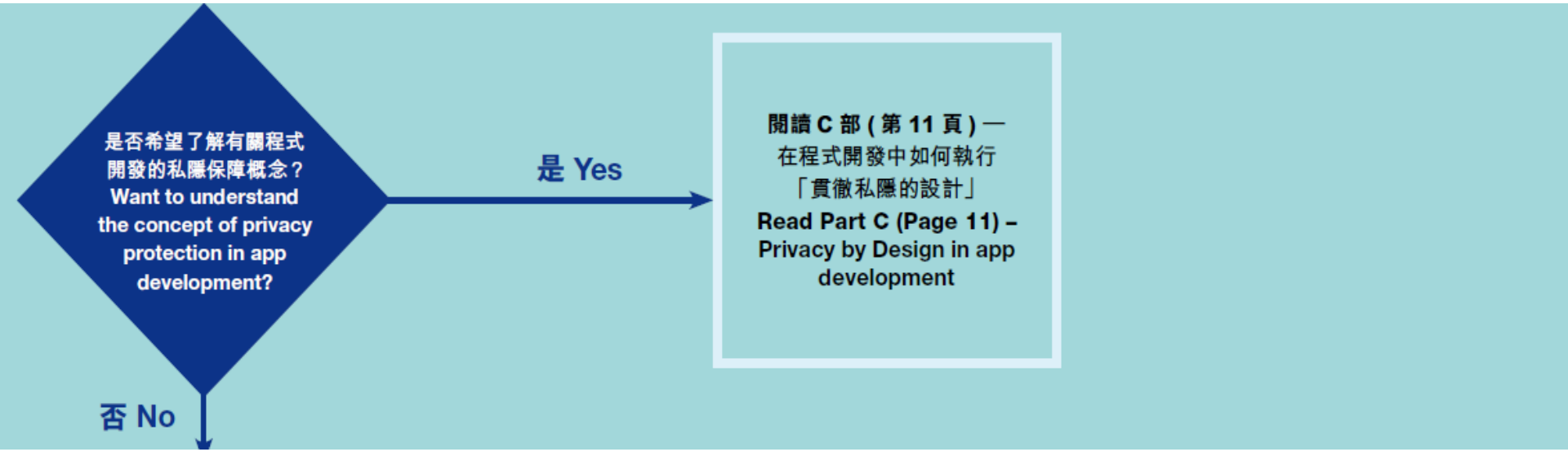
Best Practice Guide for Mobile App Development:
Modular and flow-chart approach



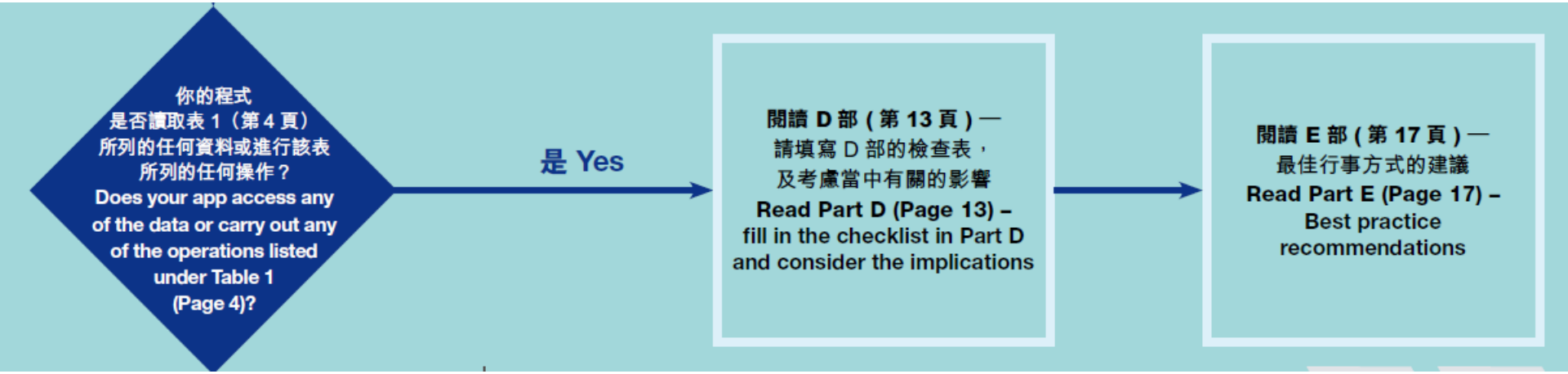
Best Practice Guide for Mobile App Development:
Legal requirements



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													

Best Practice Guide for Mobile App Development:
Transparency

Your App Could be Here Next Year as a Good Example…

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[1] 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*[6] 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.

What Next…

More practice sharing:

- PISA – How to properly implement encryption?
- HKCERT – How to manage security in mobile apps?
- PolyU – How to do a ‘black-box’ check?

Privacy by Design and Best Practice Guide on Mobile App Development