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**

**DPPs:**

1. **Collection**
2. **Accuracy and retention**
3. **Use**
4. **Security**
5. **Transparency**
6. **Rights of access and correction**
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/
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...
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

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 address¹ 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

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

何時閱讀
WHEN TO READ

你應在開始計劃開發程式時便閱讀本指引。對企業來說，在開始階段便融入保障私隱的神想，可相抵於未來才作出這方面的調整，將來的修改會較少，而對程式功能的影響亦較為輕微。

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

為方便閱讀，本指引由幾個部分組成，每一部分均可獨立閱讀。有關本指引的使用，可參考封面的流程表的建議。

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.

開始
Start

你的程式
Your app

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start

開始
Start
Best Practice Guide for Mobile App Development: Legal requirements

開始 Start

對私隱保障是否不太熟悉並希望知道更多私隱法例？
New to privacy protection and want to know more on privacy law?

否 No

是 Yes

閱讀 A 部 (第 6 頁) —
《個人資料（私隱）條例》的
相關性
Read Part A (Page 6) —
The relevance of the Personal Data (Privacy) Ordinance

閱讀 B 部 (第 8 頁) —
法例有甚麼要求？
Read Part B (Page 8) —
What are the requirements under the law?
Best Practice Guide for Mobile App Development: 
*Privacy by Design explained*

是否希望了解有關程式開發的私隱保護概念？
Want to understand the concept of privacy protection in app development?

是 Yes

否 No

閱讀C部（第11頁）—
在程式開發中如何執行「貫徹私隱的設計」
Read Part C (Page 11) – Privacy by Design in app development
Best Practice Guide for Mobile App Development:

Best practice recommendations
### Best Practice Guide for Mobile App Development: Checklist for self-evaluation

<table>
<thead>
<tr>
<th>Problem</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Is the access/collection/use of the data absolutely necessary for the app’s operation? See E1</td>
</tr>
<tr>
<td>2.</td>
<td>Will the data (or derived data) be uploaded/transmitted from the mobile device? See E2</td>
</tr>
<tr>
<td>3.</td>
<td>Will the data (or derived data) be stored or kept elsewhere from the mobile device? See E3</td>
</tr>
<tr>
<td>4.</td>
<td>Will the data (or derived data) be combined/correlated with other data of the individual obtained elsewhere? See E4</td>
</tr>
<tr>
<td>5.</td>
<td>Will the data (or derived data) be shared within your business (e.g. for cross-app integrations or with other partners)? See E5</td>
</tr>
<tr>
<td>6.</td>
<td>Will the data (or derived data) be used for profiling of individuals? See E6</td>
</tr>
<tr>
<td>7.</td>
<td>Will the data (or derived data) be used for direct marketing? See E7</td>
</tr>
<tr>
<td>8.</td>
<td>Has a Personal Information Collection Statement and/or Privacy Policy Statement been prepared to cover all data types involved? See E8</td>
</tr>
<tr>
<td>9.</td>
<td>Have you taken into account app users’ privacy expectations? See E9</td>
</tr>
<tr>
<td>10.</td>
<td>Do you use third-party tools (e.g., libraries, ad networks) and provide the providers of these tools today? See E10</td>
</tr>
</tbody>
</table>

---

**Table 2: Checklist**

<table>
<thead>
<tr>
<th>Problem</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Is the access/collection/use of the data absolutely necessary for the app’s operation? See E1</td>
</tr>
<tr>
<td>2.</td>
<td>Will the data (or derived data) be uploaded/transmitted from the mobile device? See E2</td>
</tr>
<tr>
<td>3.</td>
<td>Will the data (or derived data) be stored or kept elsewhere from the mobile device? See E3</td>
</tr>
<tr>
<td>4.</td>
<td>Will the data (or derived data) be combined/correlated with other data of the individual obtained elsewhere? See E4</td>
</tr>
<tr>
<td>5.</td>
<td>Will the data (or derived data) be shared within your business (e.g. for cross-app integrations or with other partners)? See E5</td>
</tr>
<tr>
<td>6.</td>
<td>Will the data (or derived data) be used for profiling of individuals? See E6</td>
</tr>
<tr>
<td>7.</td>
<td>Will the data (or derived data) be used for direct marketing? See E7</td>
</tr>
<tr>
<td>8.</td>
<td>Has a Personal Information Collection Statement and/or Privacy Policy Statement been prepared to cover all data types involved? See E8</td>
</tr>
<tr>
<td>9.</td>
<td>Have you taken into account app users’ privacy expectations? See E9</td>
</tr>
<tr>
<td>10.</td>
<td>Do you use third-party tools (e.g., libraries, ad networks) and provide the providers of these tools today? See E10</td>
</tr>
</tbody>
</table>
Best Practice Guide for Mobile App Development: Transparency

你的程式是否讀取表 1（第 4 頁）所列的任何資料或進行該表所列的任何操作？
Does your app access any of the data or carry out any of the operations listed under Table 1 (Page 4)?

否 No

否 No

你的程式未必會引起個人資料私隱的問題，但請參閱及考慮 F 部 (第 28 頁) 的建議
Your app may not raise personal data privacy concerns but read and consider the recommendations in Part F (Page 28)
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