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
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 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 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").
Issues identified in the past

Lack of options/opt-out

A  Yes □
B  Yes □
C  Yes □
D  Yes □
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

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

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 - 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?

Your WhatsApp code is 542-828 but you can simply tap on this link to verify your device:

v.whatsapp.com/542828
Best Practice Guide for Mobile App Development

Best Practice Guide for Mobile App Development

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

Legal requirements

開始
Start

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

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

否 No

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
### Table 2 - Checklist

<table>
<thead>
<tr>
<th>項目</th>
<th>問題</th>
<th>資料類別</th>
<th>當然</th>
<th>事項及運作</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>是否編製應用程式/GUI之使用者識別？</td>
<td>資料</td>
<td>使用者</td>
<td>collide/ID</td>
</tr>
<tr>
<td>2.</td>
<td>是否已將應用程式之使用者等級資料（例如使用者資料）所載</td>
<td>資料</td>
<td>使用者</td>
<td>collide/ID</td>
</tr>
<tr>
<td>3.</td>
<td>是否有為應用程式之使用者等級資料之储存/傳輸</td>
<td>資料</td>
<td>使用者</td>
<td>collide/ID</td>
</tr>
<tr>
<td>4.</td>
<td>是否有為應用程式之使用者等級資料之儲存/傳輸</td>
<td>資料</td>
<td>使用者</td>
<td>collide/ID</td>
</tr>
<tr>
<td>5.</td>
<td>是否有為應用程式之使用者等級資料之儲存/傳輸</td>
<td>資料</td>
<td>使用者</td>
<td>collide/ID</td>
</tr>
<tr>
<td>6.</td>
<td>是否有為應用程式之使用者等級資料之儲存/傳輸</td>
<td>資料</td>
<td>使用者</td>
<td>collide/ID</td>
</tr>
<tr>
<td>7.</td>
<td>是否有為應用程式之使用者等級資料之儲存/傳輸</td>
<td>資料</td>
<td>使用者</td>
<td>collide/ID</td>
</tr>
<tr>
<td>8.</td>
<td>是否已將應用程式之使用者等級資料之儲存/傳輸</td>
<td>資料</td>
<td>使用者</td>
<td>collide/ID</td>
</tr>
<tr>
<td>9.</td>
<td>是否已將應用程式之使用者等級資料之儲存/傳輸</td>
<td>資料</td>
<td>使用者</td>
<td>collide/ID</td>
</tr>
<tr>
<td>10.</td>
<td>是否已將應用程式之使用者等級資料之儲存/傳輸</td>
<td>資料</td>
<td>使用者</td>
<td>collide/ID</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>問題</th>
<th>得以使用</th>
<th>資料類別</th>
<th>當然</th>
<th>事項及運作</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>是否編製應用程式/GUI之使用者識別？</td>
<td>資料</td>
<td>使用者</td>
<td>collide/ID</td>
</tr>
<tr>
<td>2.</td>
<td>是否已將應用程式之使用者等級資料（例如使用者資料）所載</td>
<td>資料</td>
<td>使用者</td>
<td>collide/ID</td>
</tr>
<tr>
<td>3.</td>
<td>是否有為應用程式之使用者等級資料之儲存/傳輸</td>
<td>資料</td>
<td>使用者</td>
<td>collide/ID</td>
</tr>
<tr>
<td>4.</td>
<td>是否有為應用程式之使用者等級資料之儲存/傳輸</td>
<td>資料</td>
<td>使用者</td>
<td>collide/ID</td>
</tr>
<tr>
<td>5.</td>
<td>是否有為應用程式之使用者等級資料之儲存/傳輸</td>
<td>資料</td>
<td>使用者</td>
<td>collide/ID</td>
</tr>
<tr>
<td>6.</td>
<td>是否有為應用程式之使用者等級資料之儲存/傳輸</td>
<td>資料</td>
<td>使用者</td>
<td>collide/ID</td>
</tr>
<tr>
<td>7.</td>
<td>是否有為應用程式之使用者等級資料之儲存/傳輸</td>
<td>資料</td>
<td>使用者</td>
<td>collide/ID</td>
</tr>
<tr>
<td>8.</td>
<td>是否已將應用程式之使用者等級資料之儲存/傳輸</td>
<td>資料</td>
<td>使用者</td>
<td>collide/ID</td>
</tr>
<tr>
<td>9.</td>
<td>是否已將應用程式之使用者等級資料之儲存/傳輸</td>
<td>資料</td>
<td>使用者</td>
<td>collide/ID</td>
</tr>
<tr>
<td>10.</td>
<td>是否已将應用程式之使用者等級資料之儲存/傳輸</td>
<td>資料</td>
<td>使用者</td>
<td>collide/ID</td>
</tr>
</tbody>
</table>
Best Practice Guide for Mobile App Development

Transparency

Does your app access any of the data or carry out any of the operations listed under Table 1 (Page 4)?

Your app may not raise personal data privacy concerns but read and consider the recommendations in Part F (Page 28).
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 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 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