國際 INTERNATIONAL IT FEST 滙 2015
INTERACTIVE HONG KONG

Developing Mobile Apps with Privacy Protection in Mind

Henry Chang, IT Advisor
Office of the Privacy Commissioner for Personal Data, Hong Kong
15 April 2015

Developing Mobile Apps with Privacy Protection in Mind Seminar

Co-organisers & Supporting Organisations

Co-organisers:

CAHK 香港通訊業聯會 Communications Association of Hong Kong

Hong Kong Association of Interactive Marketing 香港互動市務商會

HKCERT

Hong Kong Computer Society

HKIE The Hong Kong Institution of Engineers Information Technology Division

WTIA 香港無線科技商會

ISACA China Hong Kong Chapter

iProA Internet Professional Association 互聯網專業協會

Internet Society Hong Kong 香港互聯網協會

PISA

Supporting Organisations:

香港中文大學 The Chinese University of Hong Kong Faculty of Engineering

香港浸會大學 Hong Kong Baptist University

CYBERPORT 數碼港

IVE Member of VTC Group

HKGCC Hong Kong General Chamber of Commerce

The Hong Kong Polytechnic University 香港理工大學

HKPC Hong Kong Productivity Council

Hong Kong 香港科技園 Science & Technology Parks

HKUST World Class Inside

Office of the Government Chief Information Officer

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East, Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Developing Mobile Apps with Privacy Protection in Mind

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Developing Mobile Apps with Privacy Protection in Mind

- Background
- Data Protection Principles in apps development
- Case studies on privacy-friendly mobile apps
- Best practice guide for mobile app development

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Developing Mobile Apps with Privacy Protection in Mind

The way we were…

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Surveys on the top 60 mobile apps

May 2014

- 45% without privacy policy
- 85% policies that were not tailor-made to apps
- 8% app developers had not provided sufficient details to identify themselves
- 6% not easily readable

May 2013

- 40% without privacy policy
- 92% policies that were not tailor-made to apps
- 60% app developers had not provided contact details
- 11% in в другом языке or not easily readable

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

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.

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Developing Mobile Apps with Privacy Protection in Mind

Free publicity?

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

For this reason?

太陽 | 要聞港聞 | 兩岸國際 | 財經 | 娛樂 | 副刊 | SUN 樂園 | 體育 | 馬經 | 波經

渣打手機軟件套取用戶私隱

【本報訊】智能手提電話愈來愈普遍，有Android用戶下載渣打銀行及旅遊發展局軟件時，被要求授權讀取手提電話內個人資料，包括電話簿和行事曆，甚至可操控相機。渣打銀行回應說相信是軟件設計問題，銀行無讀取用戶個人資料。

渣打銀行一個Android軟件，要求讀取手提電話內個人資料。

有市民下載渣打銀行提供銀行分行和櫃員機位置的Android軟件後發現有問題，「安裝時要求讀取我個人資料，例如電話簿、行事曆，但軟件無需要用這些資料，我覺得奇怪，所以刪除了這個軟件。」該軟件甚至要求授權控制相機功能。

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East, Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Or this reason?

CNET › News › Security & Privacy › LinkedIn's app transmits user data without their ...

LinkedIn's app transmits user data without their knowledge

iOS app collects users' calendar data and transmits it to the networking company's servers, without revealing the transmission to members, two mobile security researchers discover.

by Steven Musil | June 5, 2012 7:52 PM PDT

Follow


```
{"calendar":{"calendarOptIn":true,"values":[{"e
vents":[{"organizer":{"name":"Adi Sharabani","e
mail":"adi@skycure.com"},"id":"635D0B49-1A84-44
5E-9FCD-00F975468B90:03E3338028A54FC0945BA33119
C297A700000000000000000000000000000000","notes"
:"AT&T conference call:\n USA:1-800-225-5288\n
Passcode:4218000#","endDate":"1338559200000","s
tartDate":"1338555600000","attendees":[{"name":
"Yair Amit","email":"yair@skycure.com"}],"title
":"Confidential: Internal financial results"}]
,"timestamp":"1338498000000"}]}}
```


香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East, Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

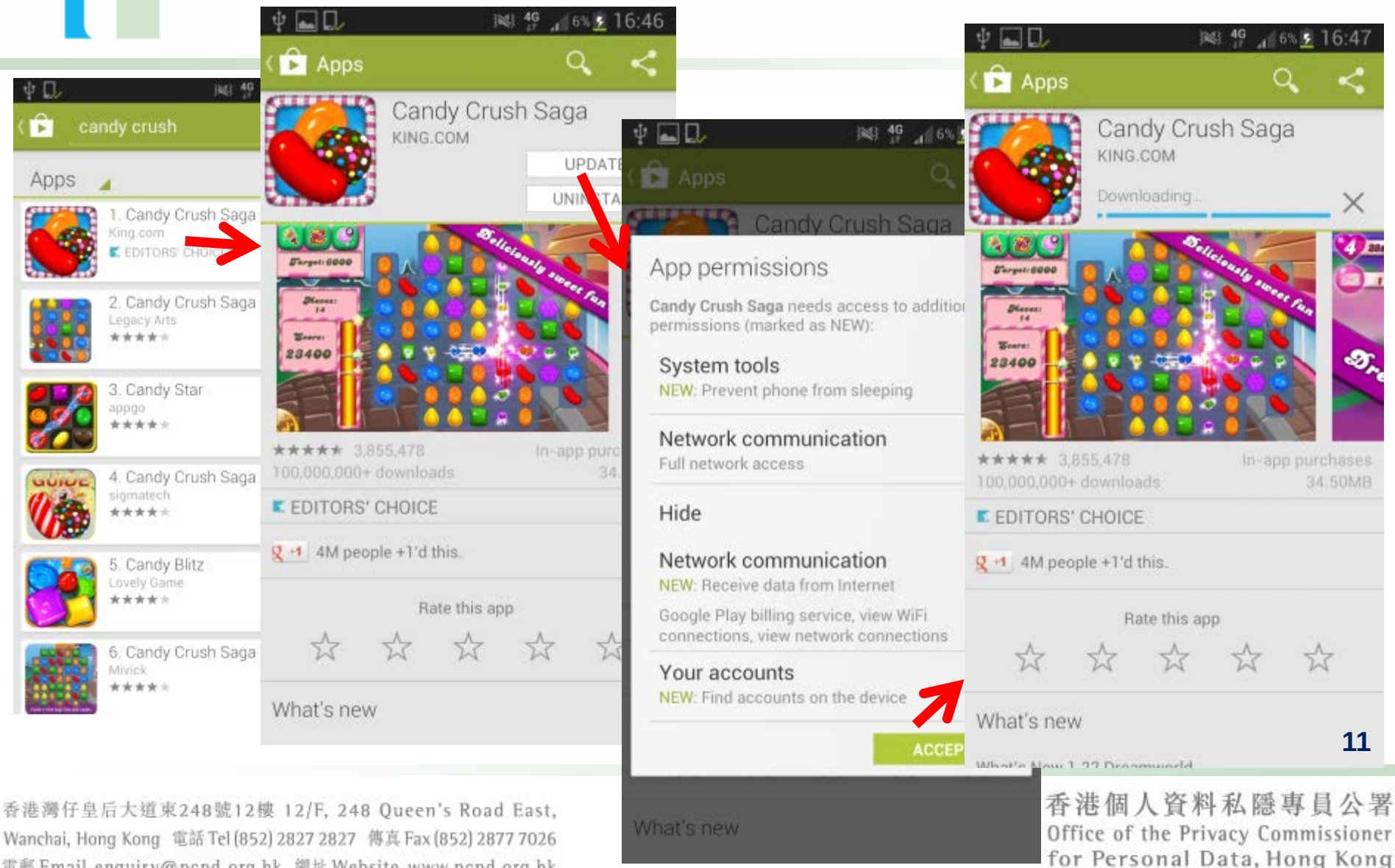
Developing Mobile Apps with Privacy Protection in Mind

Why are app users in the dark or have no control?

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

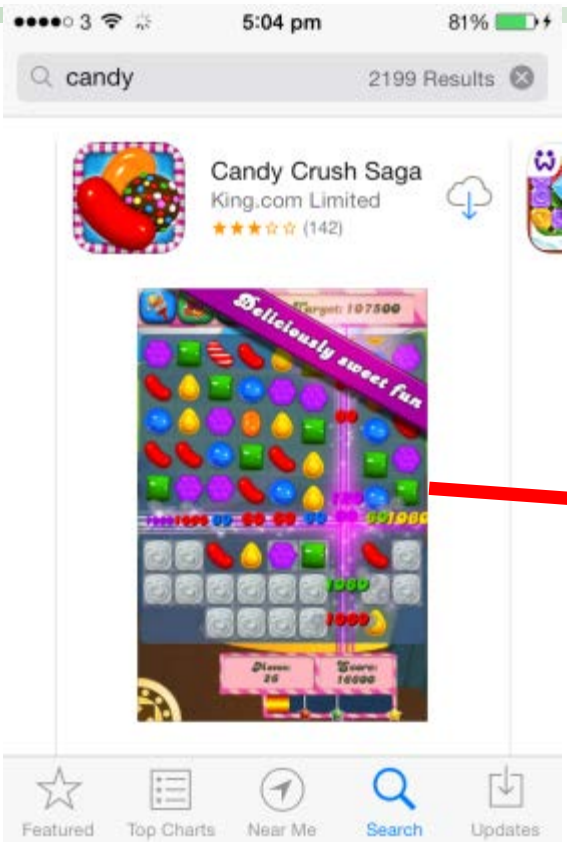
香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

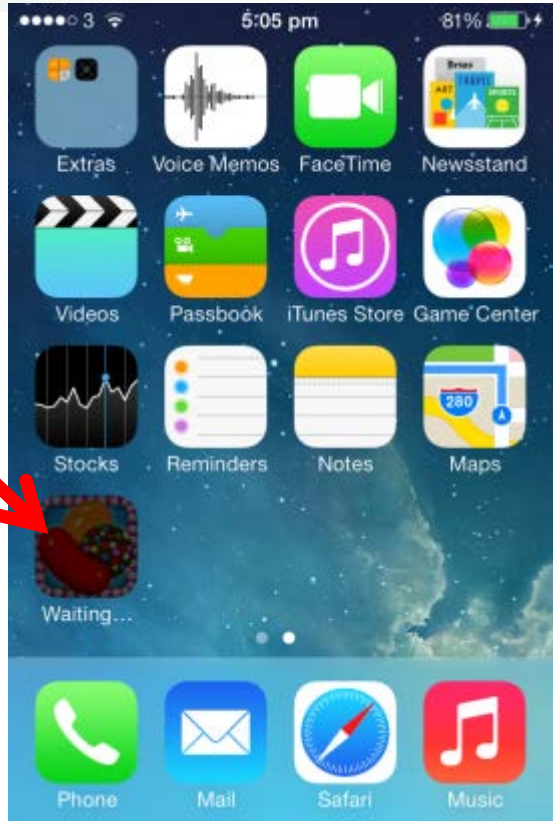
The "all-or-nothing " Android approach



香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East, Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

The "selective-control" iOS approach

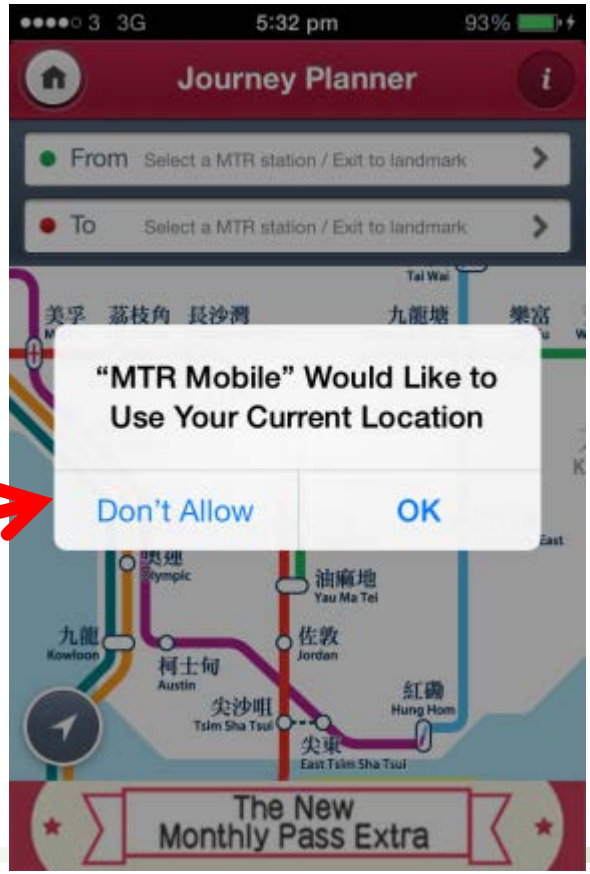


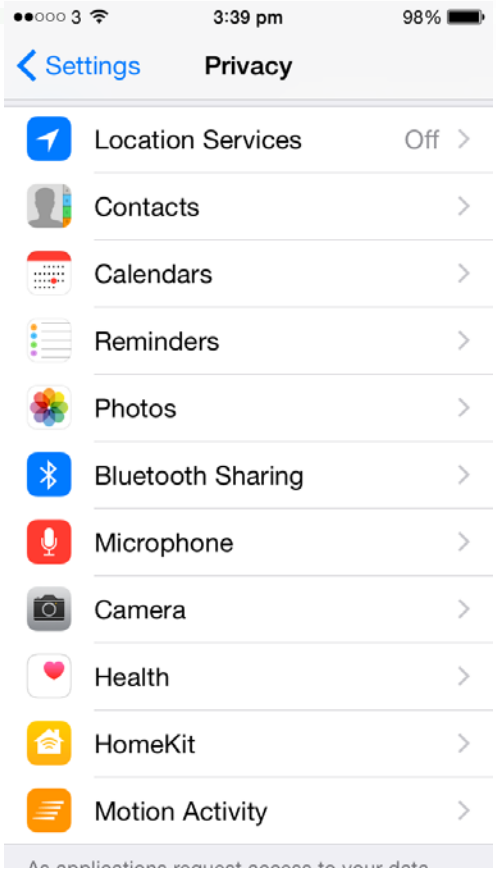


香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

The "selective-control" iOS approach





香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East, Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

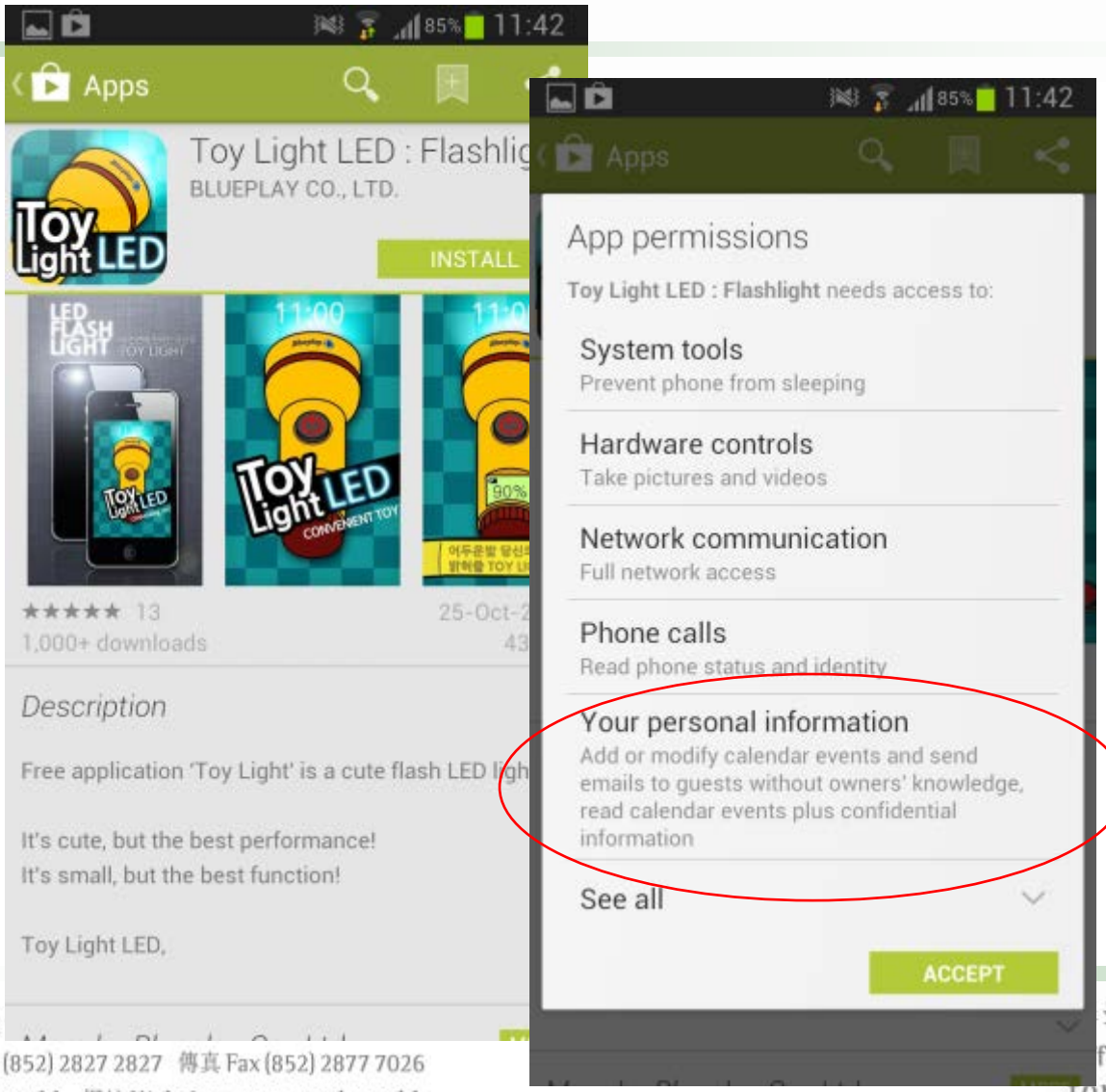
Developing Mobile Apps with Privacy Protection in Mind

Would you use these apps?

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

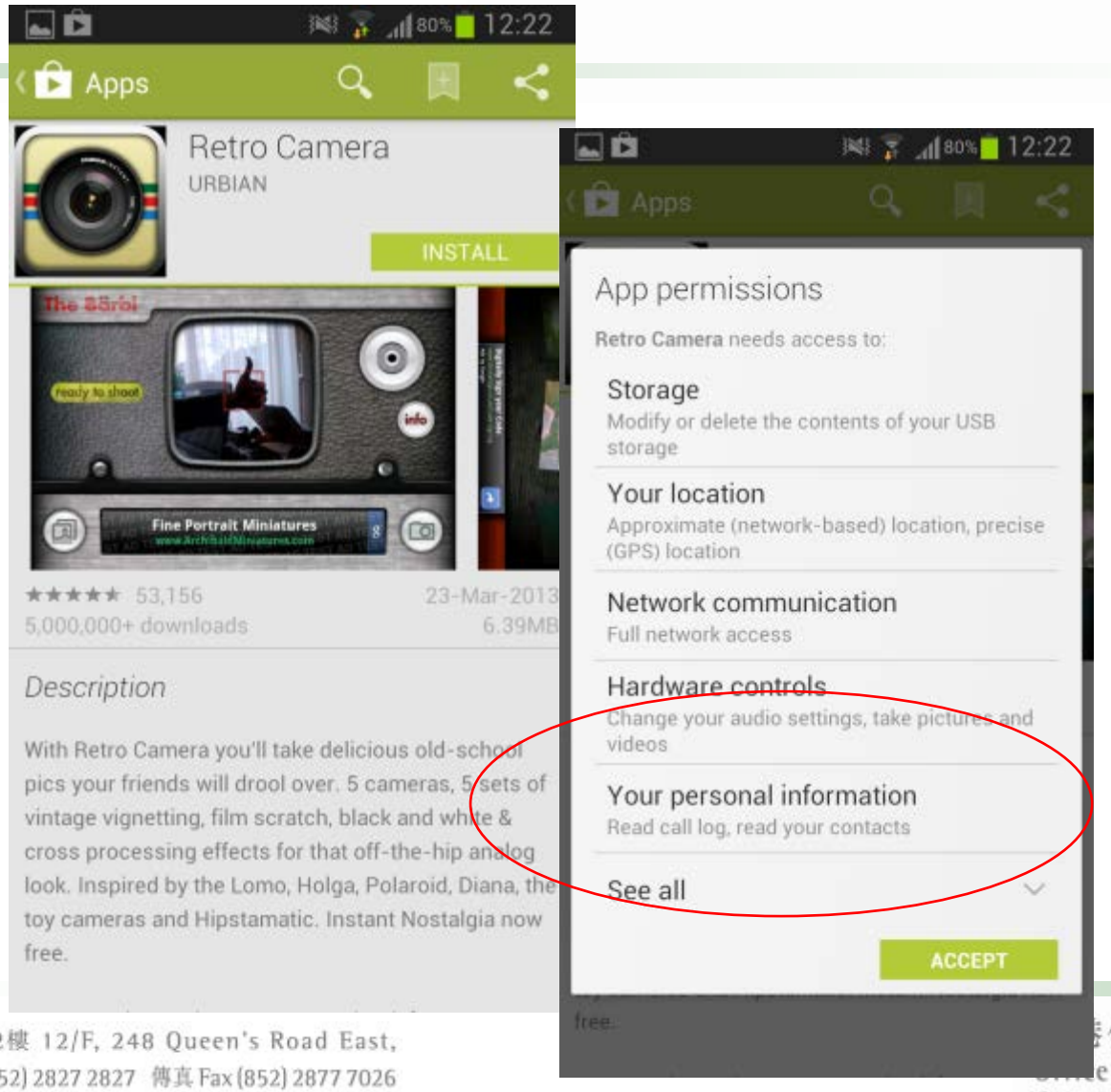
香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Would you use this app?



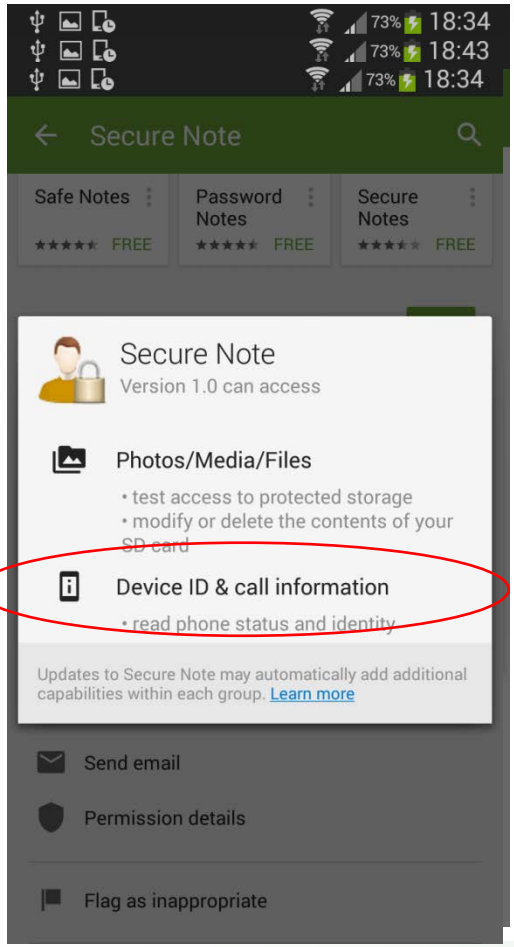
香港灣仔皇后大道東248號
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

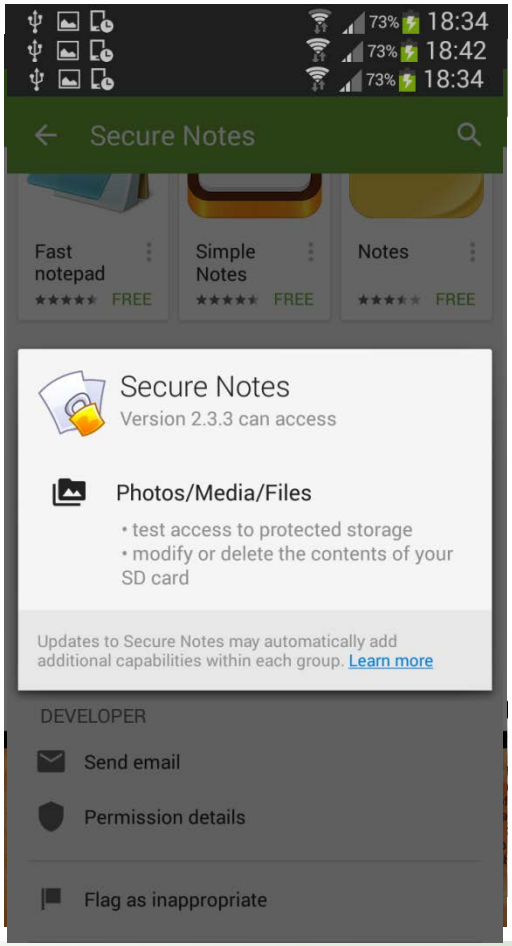
Would you use this app?

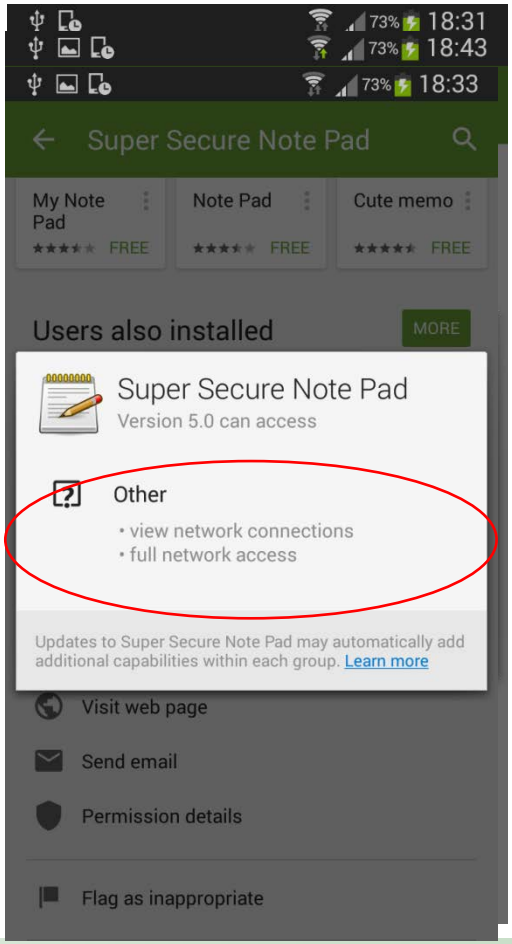


香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East, Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

Which of these apps would you install?







香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Developing Mobile Apps with Privacy Protection in Mind

What are the basic data protection principles?

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

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.

Are these personal data?

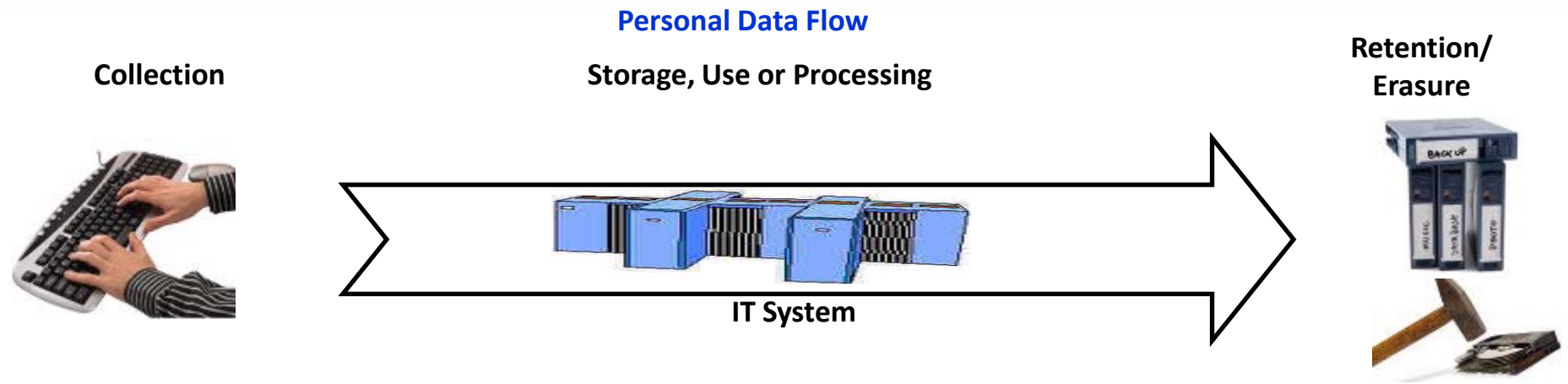
a) Email address
b) Locations
c) IMEI
d) Account names
e) Call logs
f) Contact lists

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East, Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Data Flow and Data Protection Principles (DPPs*)

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



香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

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.

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

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.

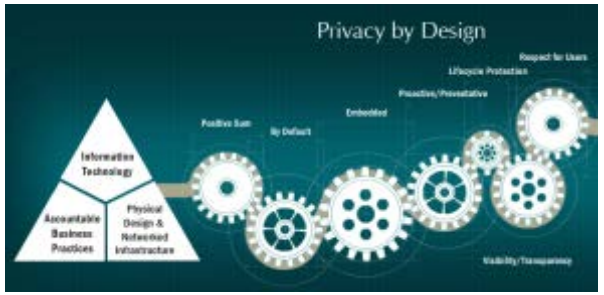
6. Access to Personal Data
   - Ensure mechanism is in place to respect the rights of data subjects for access and correction of personal data.

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

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/

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East, Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

The essence of Privacy by Design

A clever person solves problem,

a wise person avoids it.

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

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?

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Recommendations

- Whether you think you are collecting personal data, you should consider clearly stating the following details prior to app installation
  - what, when and why you are accessing the information
  - whether the information would be collected, uploaded, stored and/or shared
  - what use you have (particularly any use beyond the mobile device)
  - whether information will be combined with other information (collected at the same time or by other means) for
    - Tracking/profiling purpose
    - advertising purpose

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Mobile Application Development

Technical considerations

- 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*
- Beware of operating system features/changes
- Be familiar with mobile-specific vulnerabilities/hacking techniques
- Perform code-review and software testing

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Examples

The good, the bad and the ugly…

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

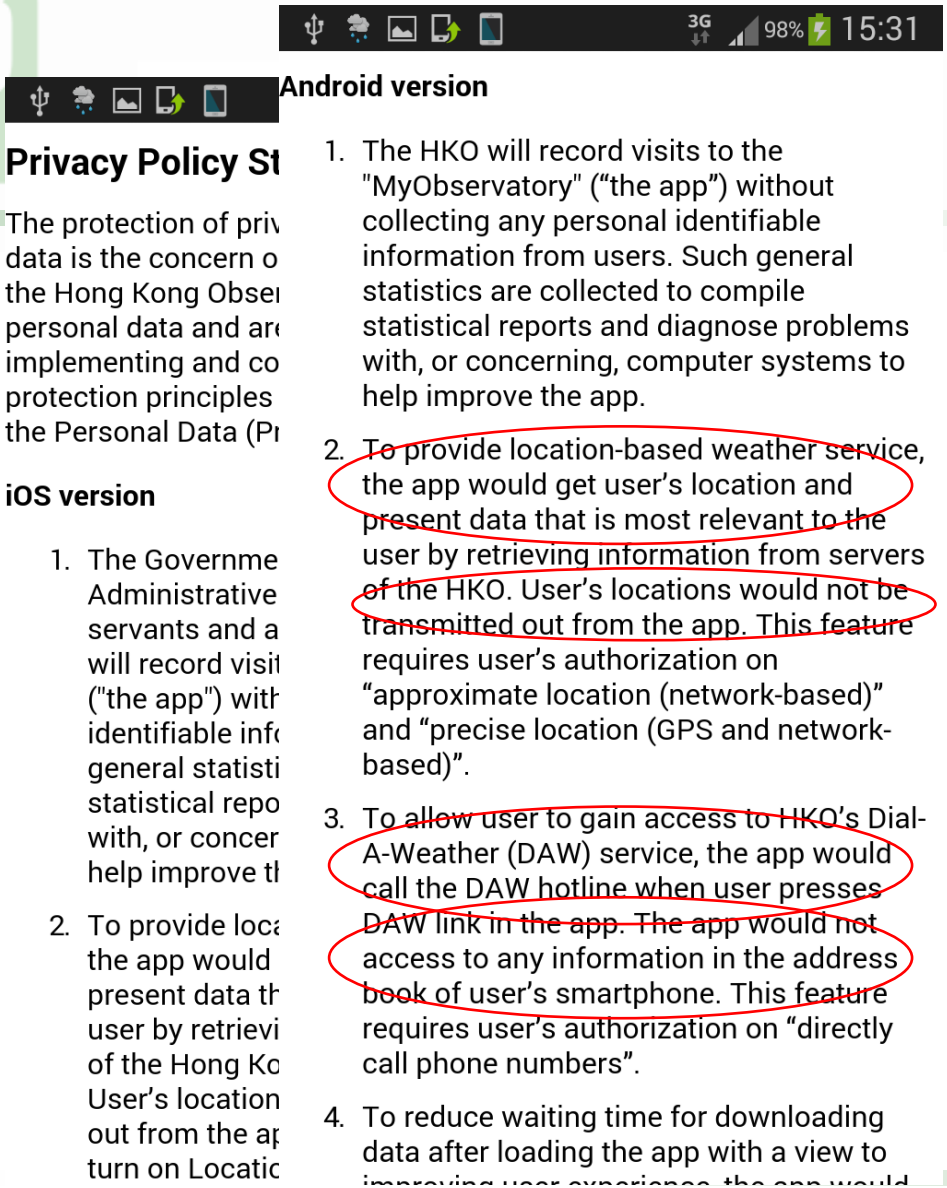
Examples

The good…

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

The good - transparent



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 info
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

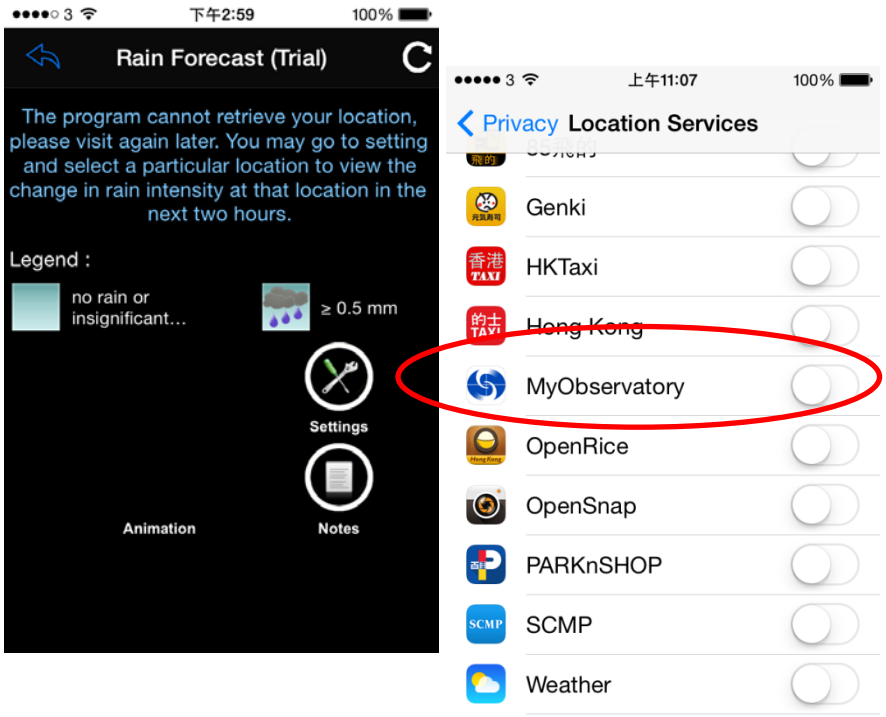
1. The HKO will record visits to the "MyObservatory" ("the app") without collecting any personal identifiable information from users. Such general statistics are collected to compile statistical reports and diagnose problems with, or concerning, computer systems to help improve the app.
2. To provide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

- **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…**

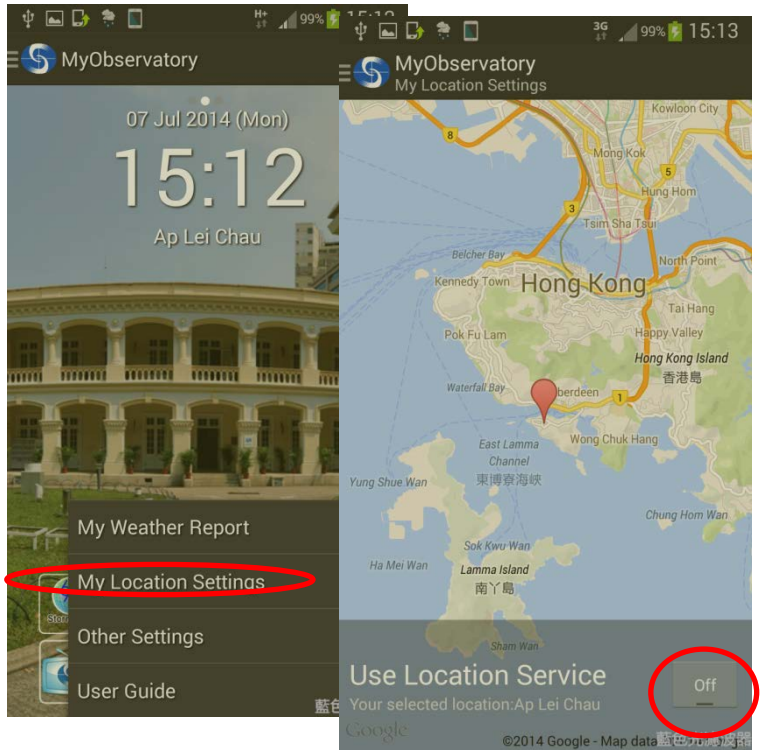
香港灣仔皇后大
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

The good - build your own granular controls

For iPhone:



Why not 'port' the logic to Android?



香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East, Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

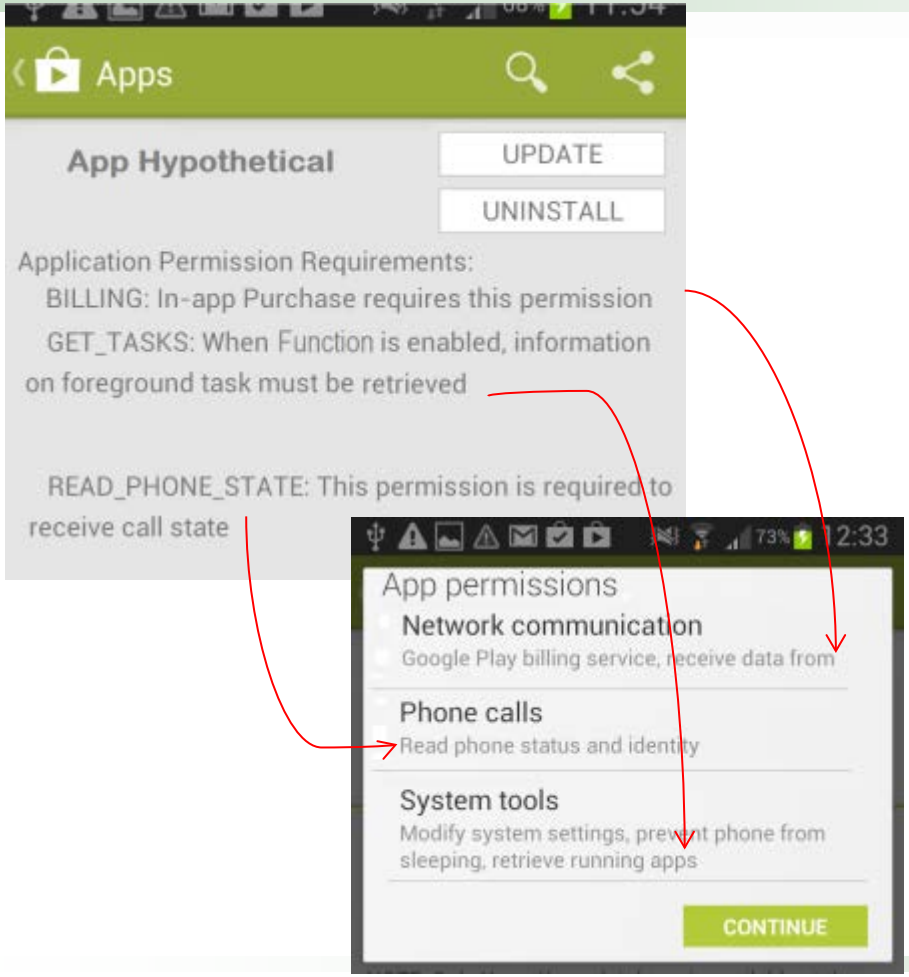
Examples

The bad...

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

The “room for improvement” – PPS transparency



- **BILLING description matches with permission sought**
- **Difficult for users to match GET_TASKS to the permission**
- **READ_PHONE_STATUS does not explain anything**
- **Concentrate on permission and neglected business purposes**
- **No explanation on advertising arrangement**

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East, Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Examples

and the ugly…

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Mistake or don't care?

Media Statements

HKA HOLIDAYS 香港航空旅遊

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[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").

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East, Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

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").

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

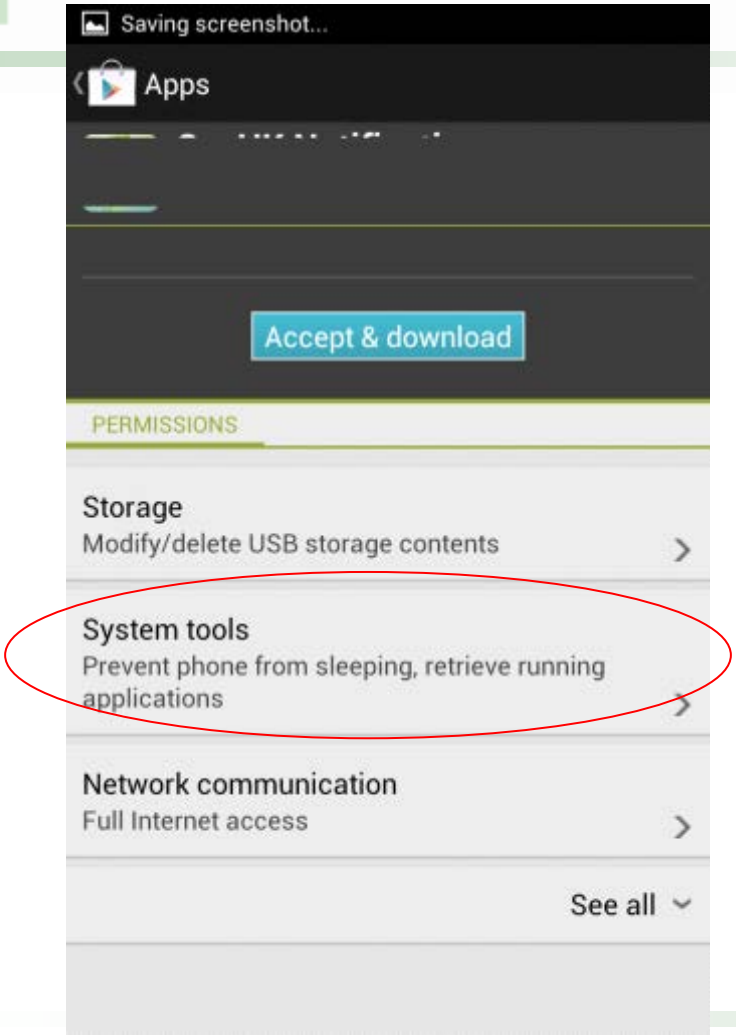
Other Recommendations

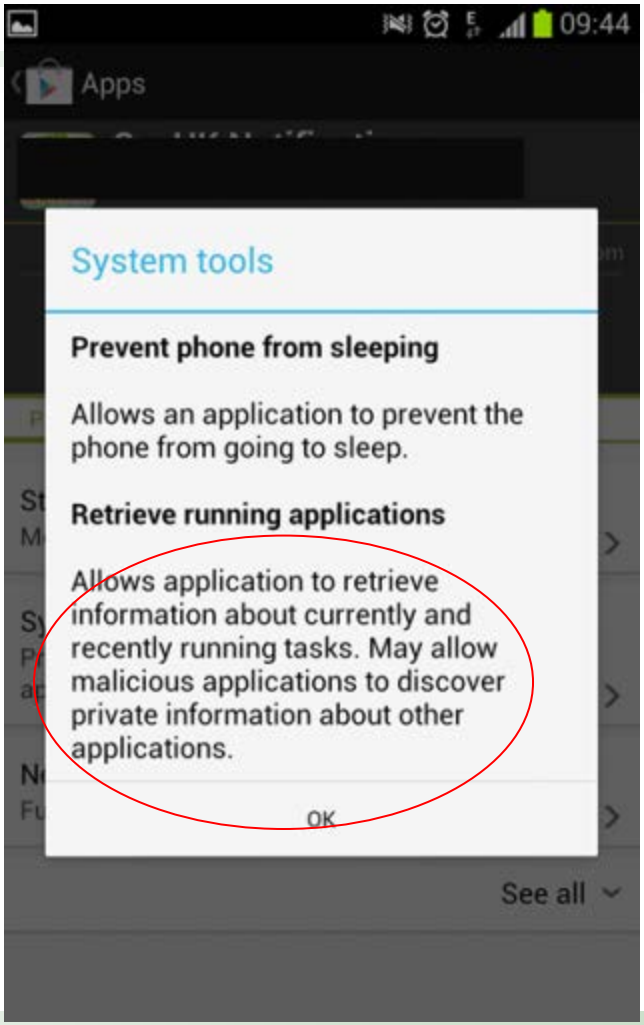
Other practical recommendations

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

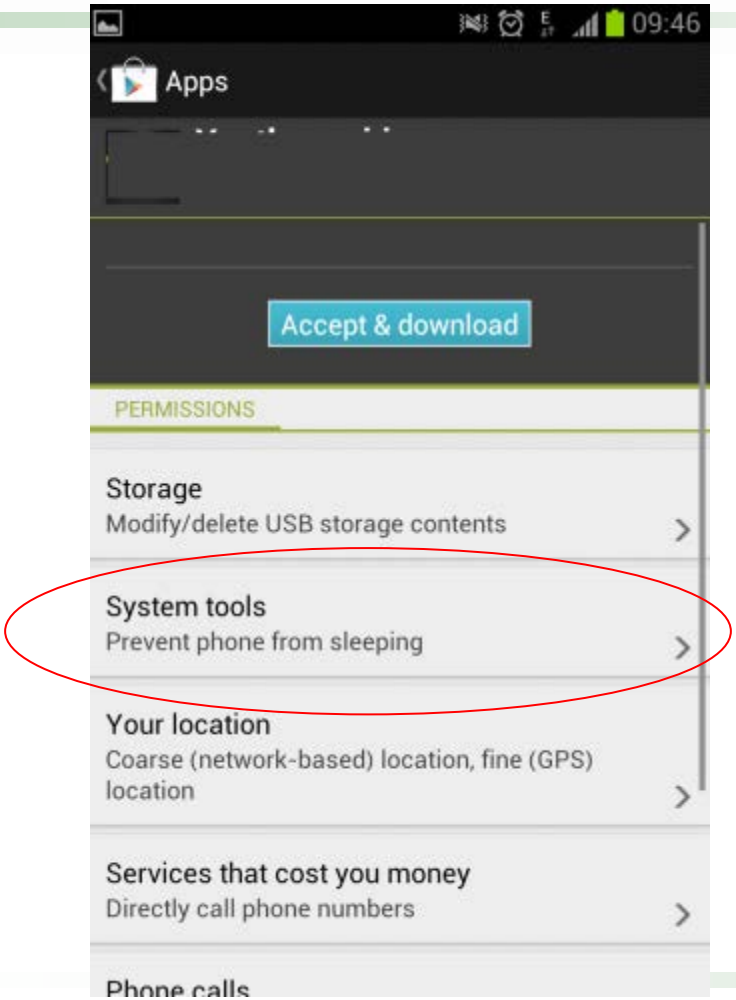
Use most specific/least privileged functions

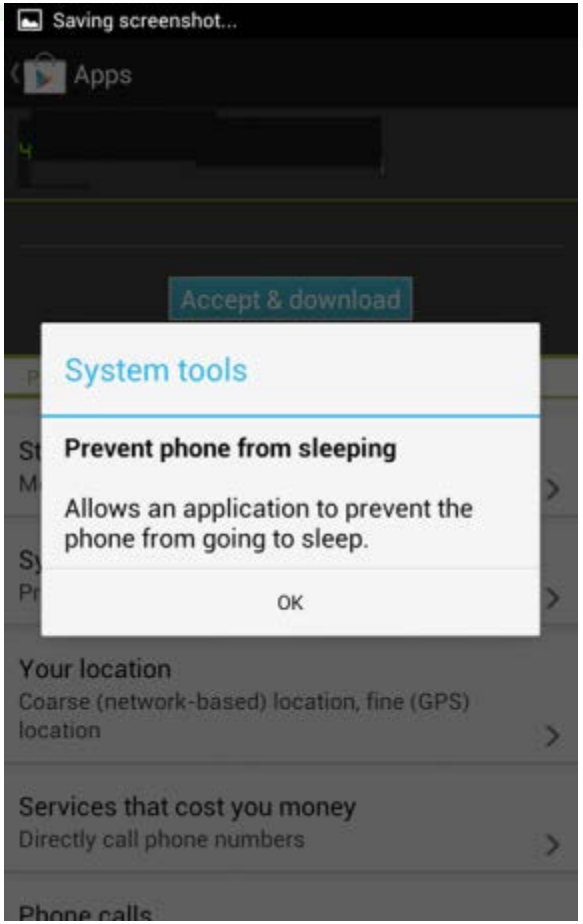




香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East, Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

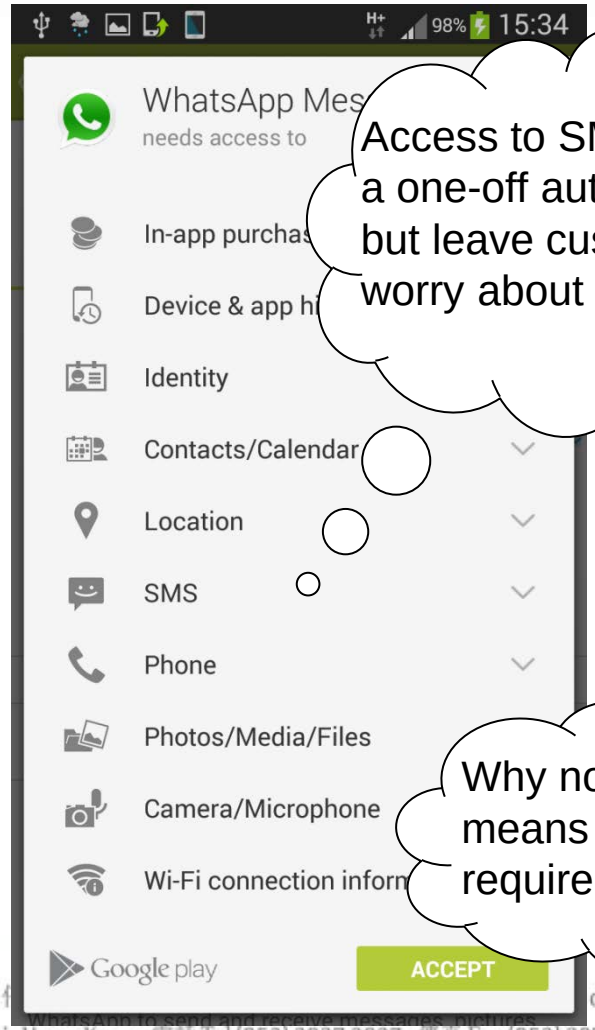
Use most specific/least privileged functions





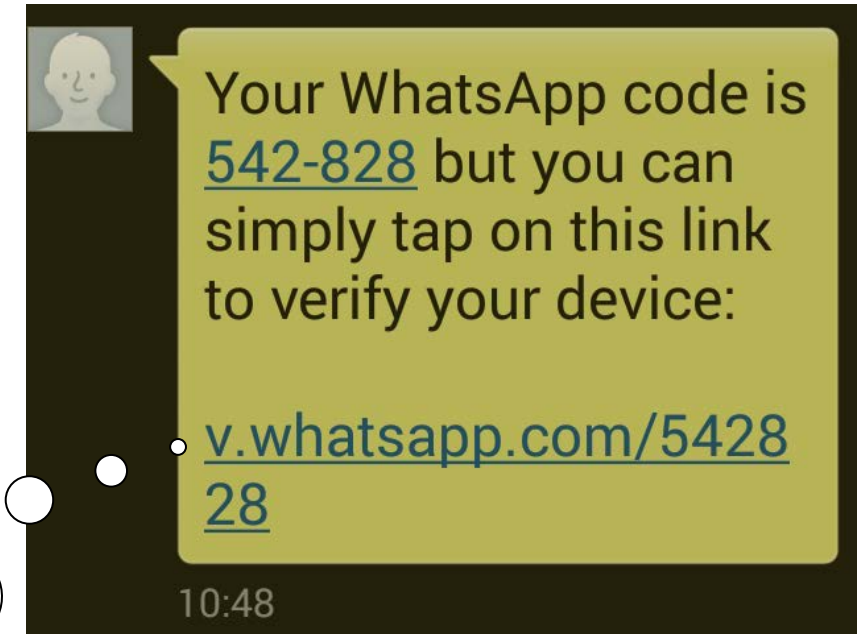
香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East, Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

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



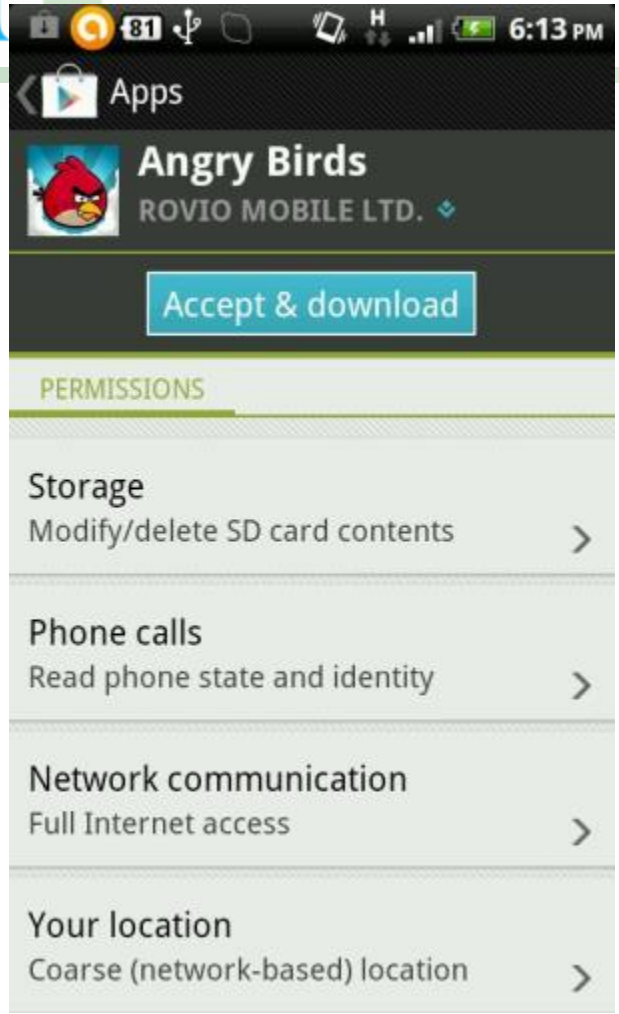
Access to SMS only for a one-off authentication but leave customers to worry about privacy.

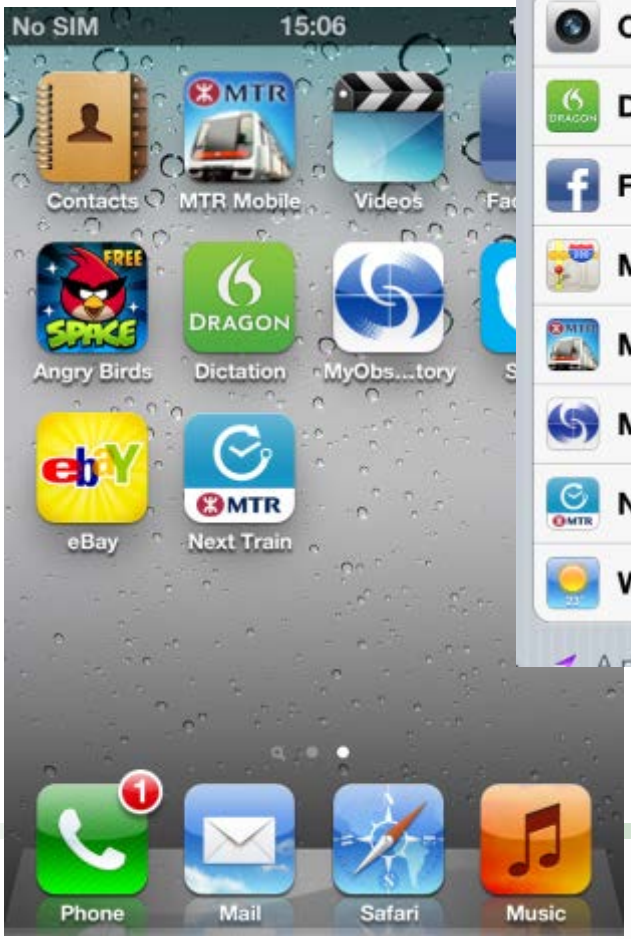
Why not use another means that would not require permission?



Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

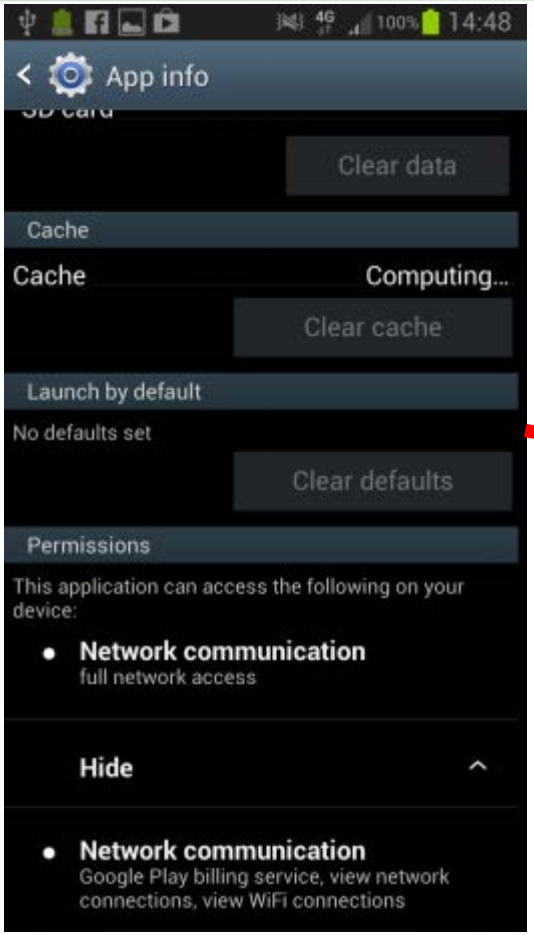
Avoid access discrepancy between Android vs iOS



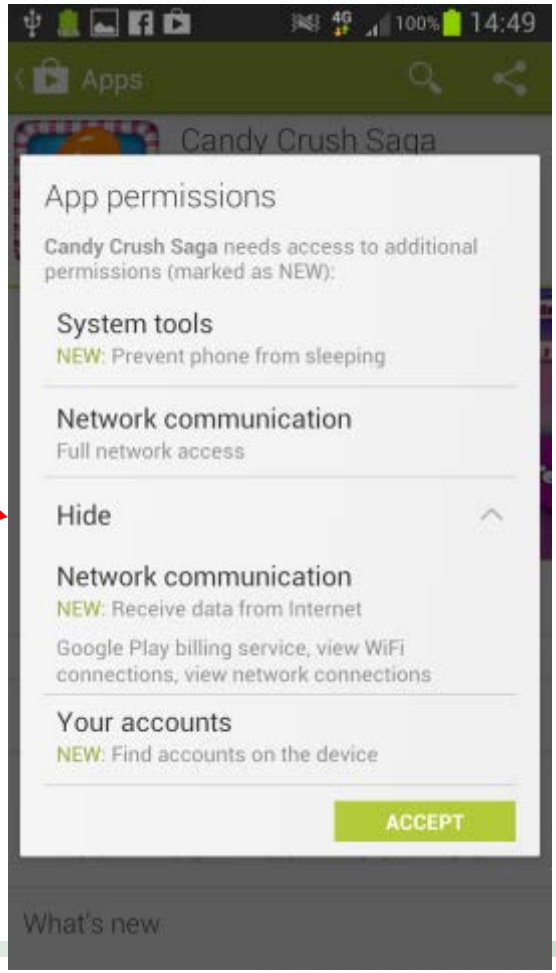


香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East, Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Avoid access creep "by the back door"?

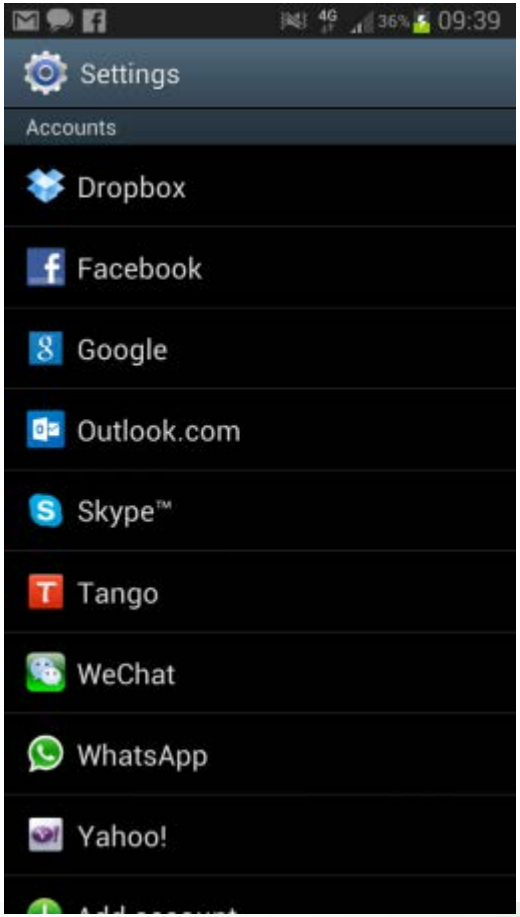


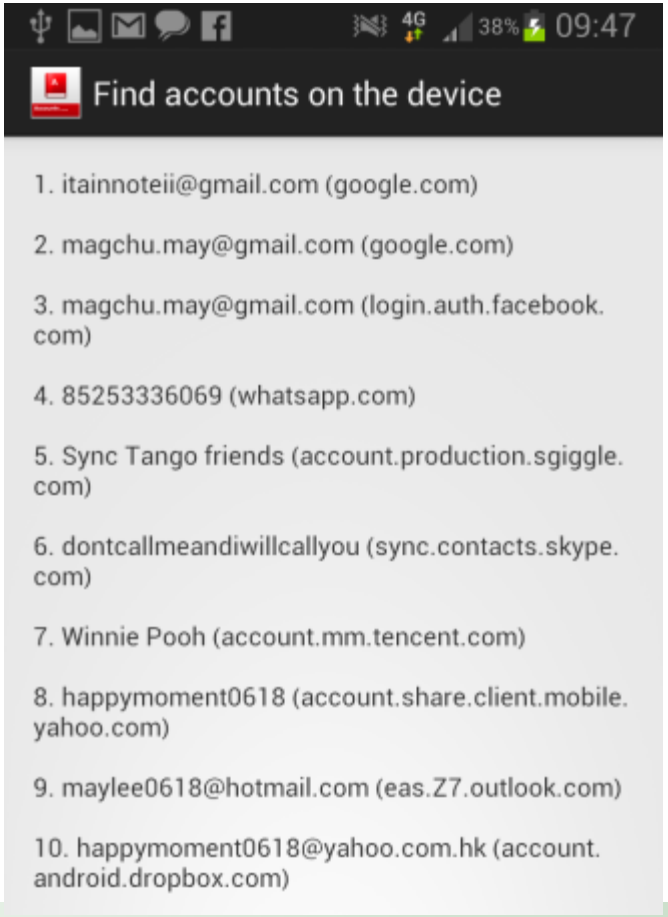
update



香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East, Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Can you justify the "Find accounts on the device" permission…



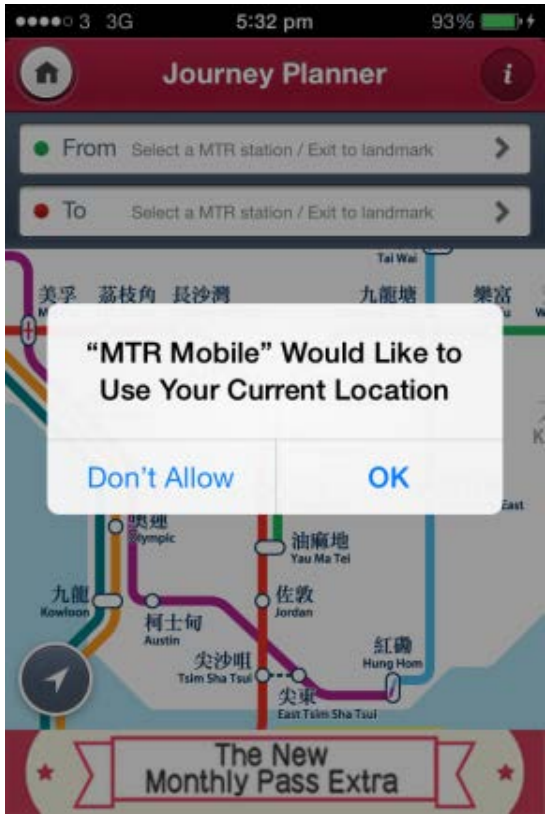


香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

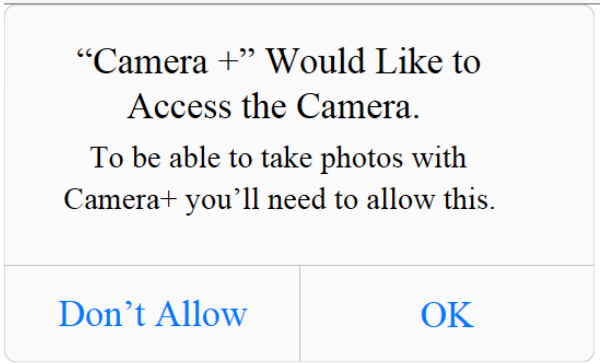
香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Make good use of iOS8's customisable "Purpose String"

Pre-iOS8



iOS8



香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East, Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Privacy and Mobile Apps Development

Please check out the "what mobile apps developers and their clients should know" leaflet

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

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

Information Leaflet

Personal data privacy protection:
what mobile apps developers and their clients should know

Introduction

This technical information leaflet aims to highlight the privacy implications that mobile applications ("**mobile apps**") developers (including organisations who commission the development of mobile apps) and operators (referred collectively as "**Developers**") should consider in developing

information such as locations travelled, photographs taken, text messages sent and received, address book contacts entered, and social network usernames and passwords used.

Normally, Apps Developers will collect personal data by directly asking mobile device users to provide their personal data. Additionally, through mobile apps, Apps Developers may access, transfer, share or supplied or device-specific data

香港灣仔皇后大道東2
Wanchai, Hong Kong 電話
電郵 Email enquiry@pc
員公署
issioner
Kong

Privacy and Transparency

Please check out the "Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement"

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

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

Guidance Note

Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement

Introduction

This Guidance Note serves as a general reference for data users when preparing Personal Information Collection Statement ("**PICS**") and Privacy Policy Statement ("**PPS**"). Both PICS and PPS are important tools used respectively for complying with the requirements of Data Protection Principle ("**DPP**")1(3) and **DPP5** under the **Personal Data (Privacy) Ordinance** (the "**Ordinance**").

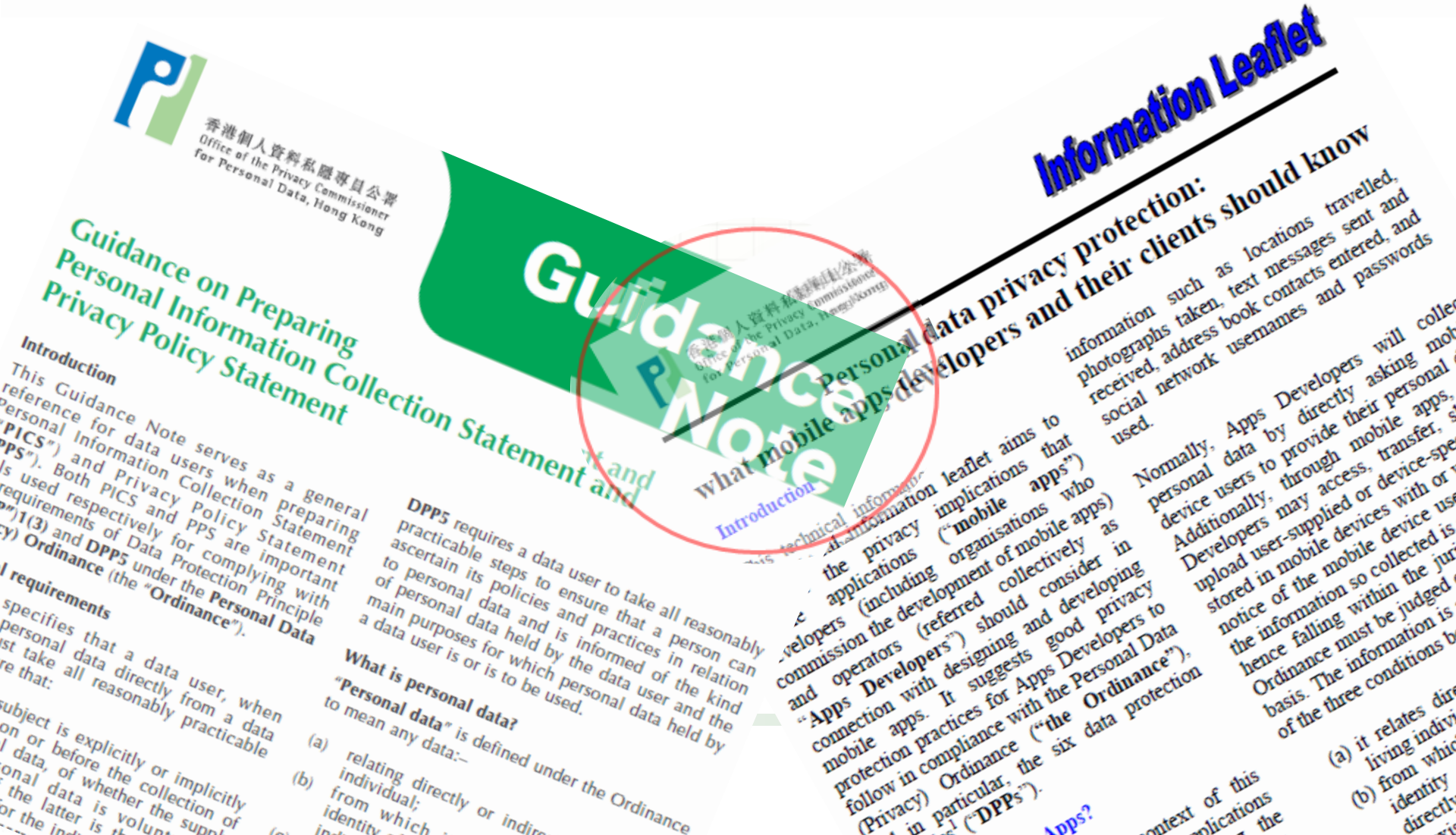
DPP5 requires a data user to take all reasonably practicable steps to ensure that a person can ascertain its policies and practices in relation to personal data and is informed of the kind of personal data held by the data user and the main purposes for which personal data held by a data user is or is to be used.

What is personal data?

香港灣仔皇后大道
Wanchai, Hong Kong
電郵 Email enquir

人資料私隱專員公署
the Privacy Commissioner
sonal Data, Hong Kong

We have only covered a small area



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

香港灣仔皇后大道東248號12樓 12/
Wanchai, Hong Kong 電話 Tel (852) 2827
電郵 Email enquiry@pcpd.org.hk 網址
員公署
issioner
Kong

Best Practice Guide for Mobile App Development:

Modular and flow-chart approach

何時閱覽
WHEN TO READ

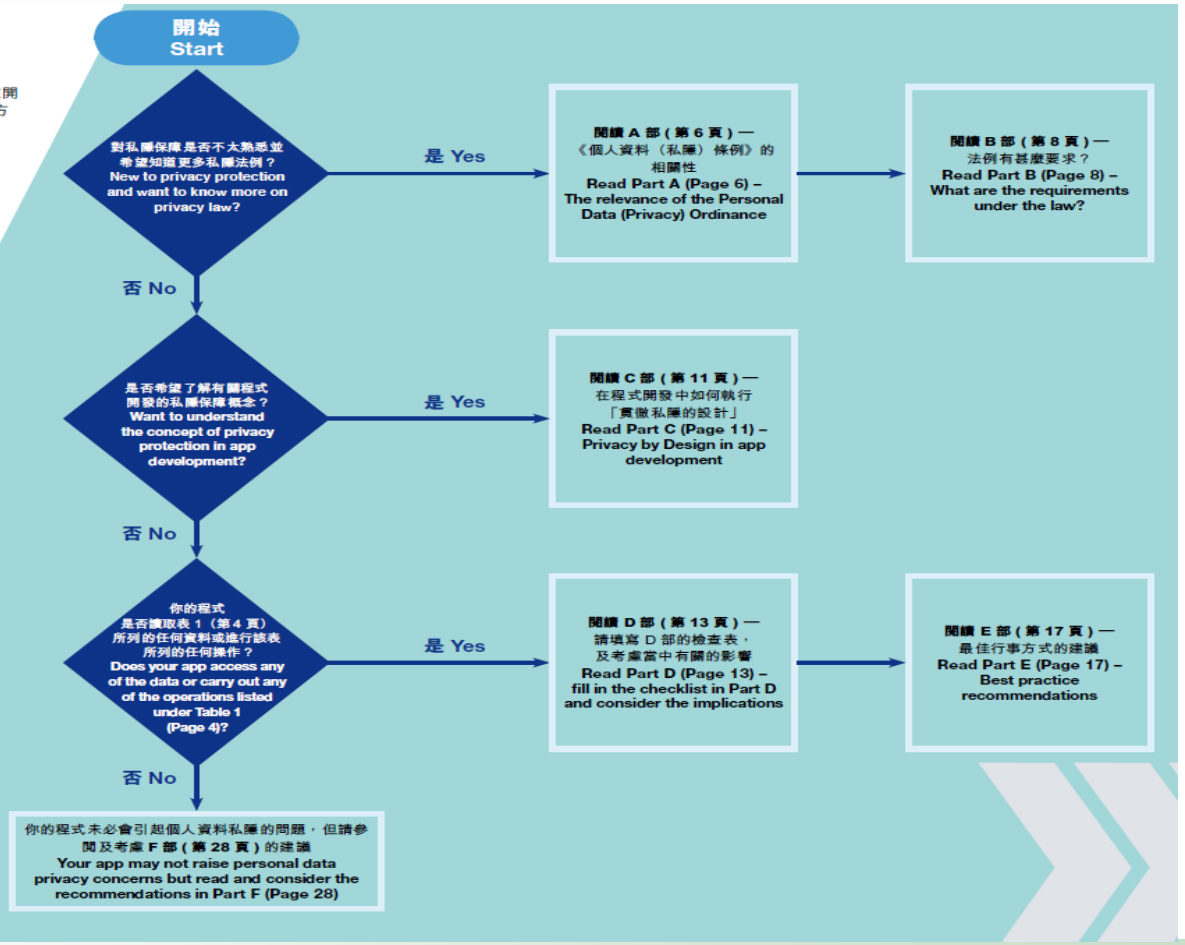
你應在開始計劃開發程式時便閱覽本指引。對企業來說，在開始階段便融入保障私隱的概念，相比日後為符規才作出這方面的調整，前者的花費會較少，而其對程式功能的影響也較為輕微。

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：

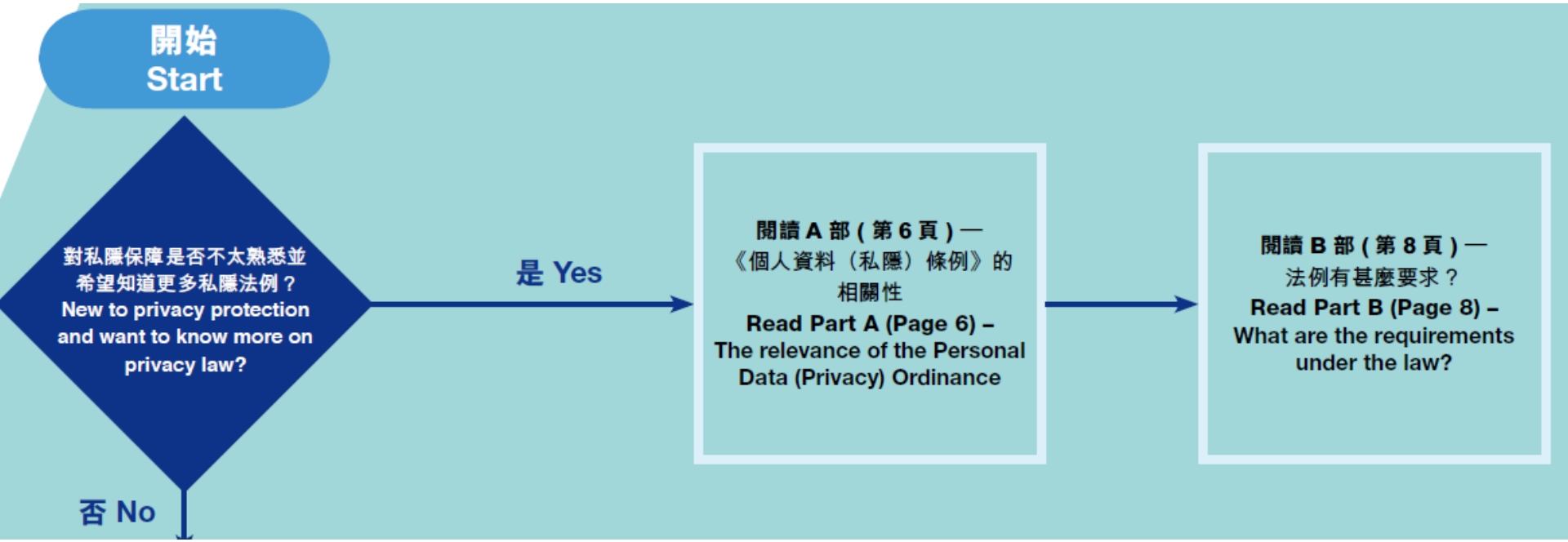
This guide comprises a number of parts which may be read independently. The flow chart on the right suggests how this guide may be used:



香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East, Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

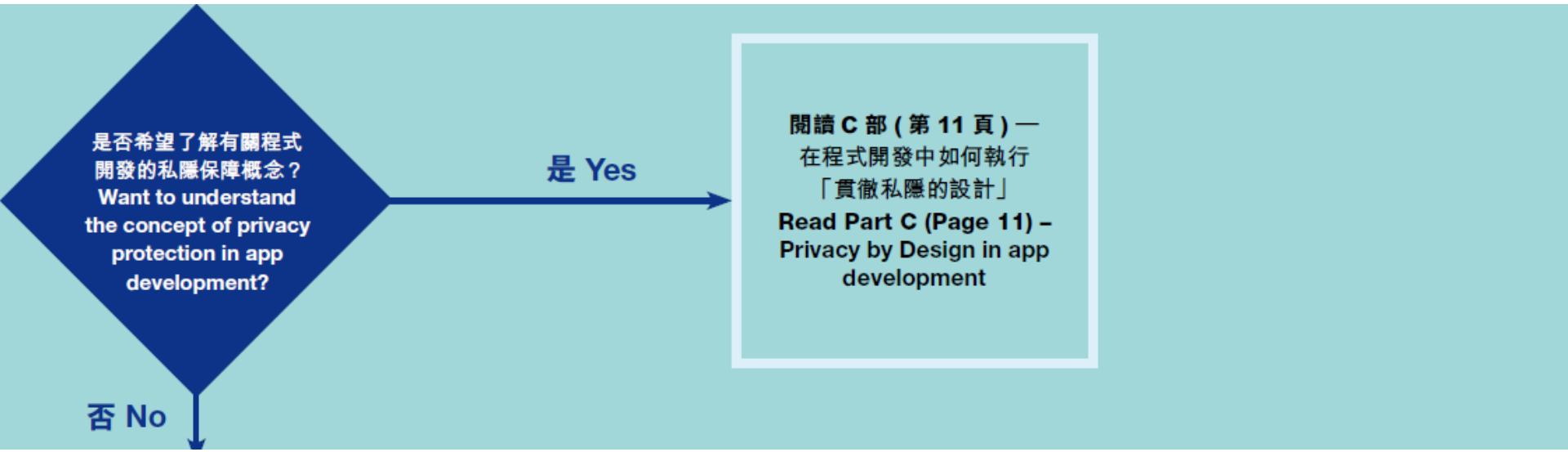
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Best Practice Guide for Mobile App Development:
Legal requirements



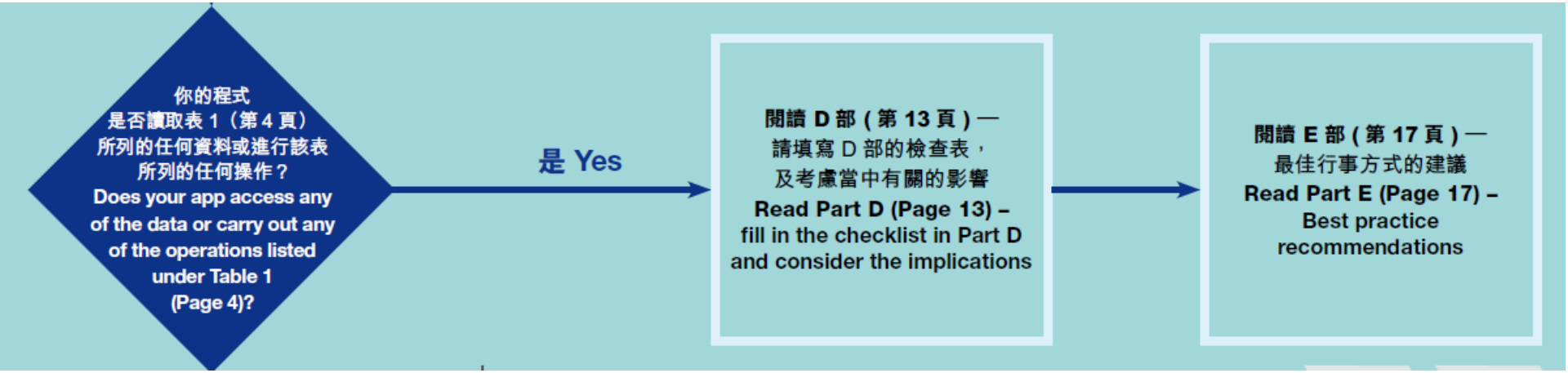
香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East, Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Best Practice Guide for Mobile App Development:
Privacy by Design explained



香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East, Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Best Practice Guide for Mobile App Development:
Best practice recommendations



香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

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		
	裝置識別碼 Unique device identifier	定位 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													

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Best Practice Guide for Mobile App Development: *Transparency*

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Your app's 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.

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Privacy Concern on Mobile App Development

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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