



流動程式私隱保障 - 使用及開發需知

個人資料私隱專員公署資訊科技顧問
張宗頤

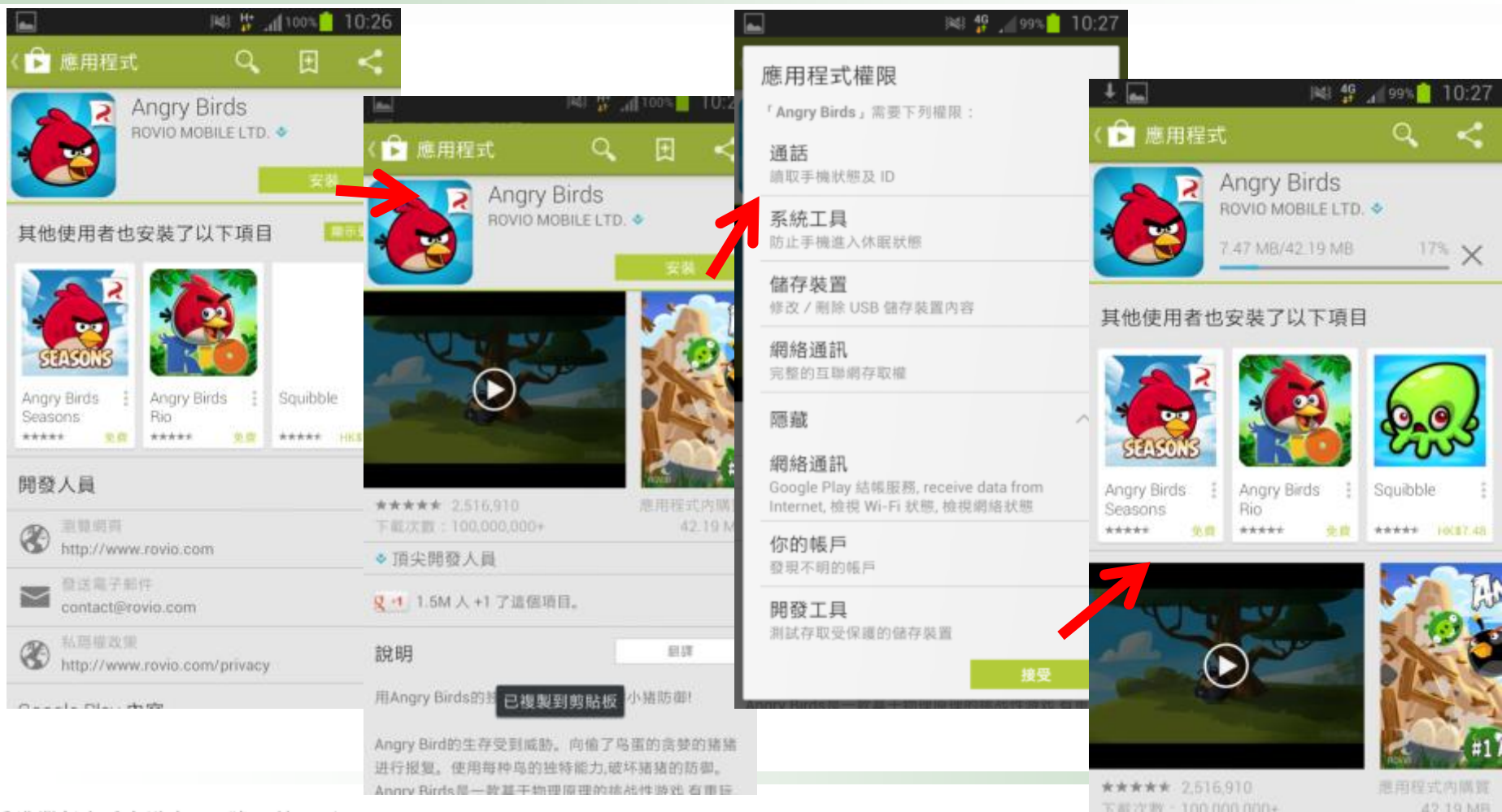


用家需知





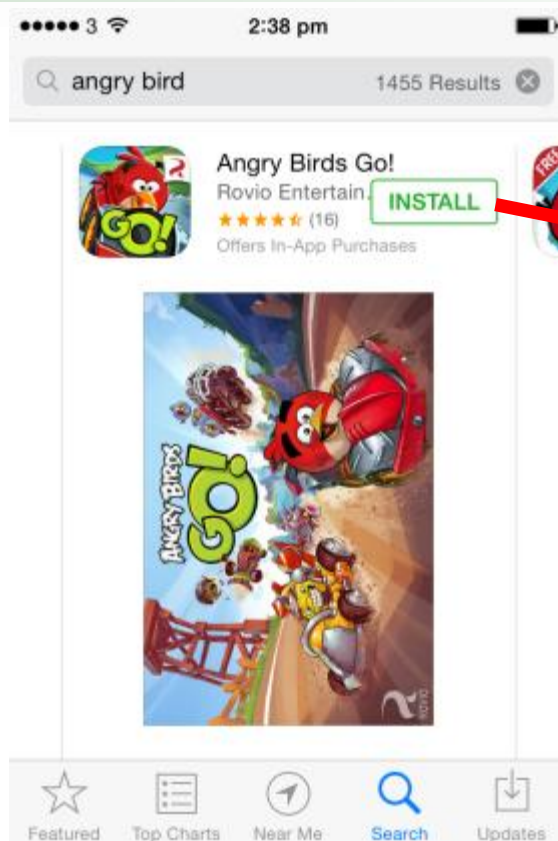
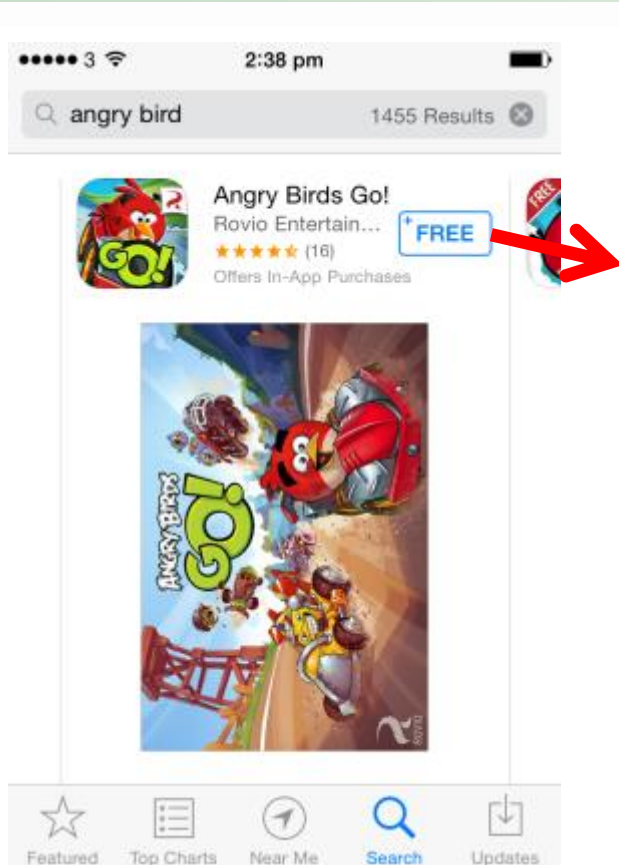
Android - 安裝前有權限顯示但不是私隱政策通知



3



iOS - 安裝前/時不通知會讀取何種資料





iOS Apps – 但讀取某些資料前會要求批准





60個熱門流動程式的抽查結果



2014年5月

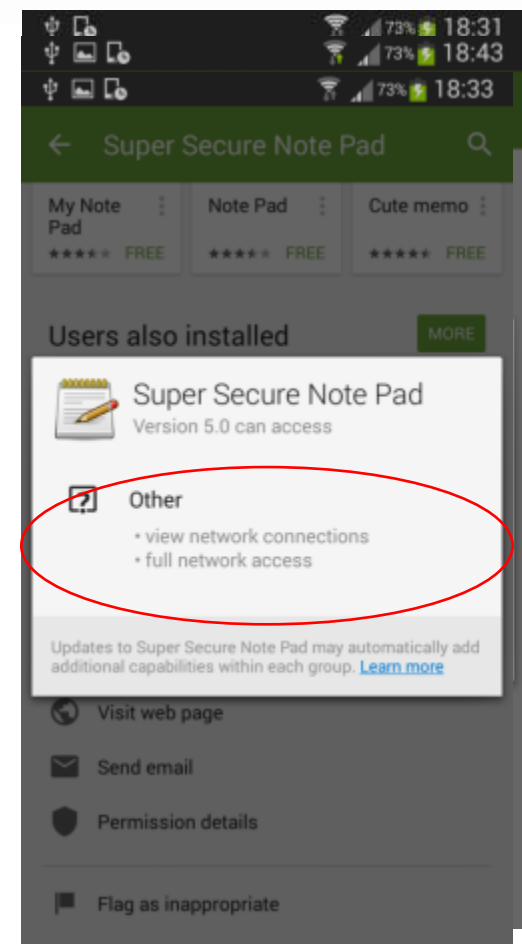
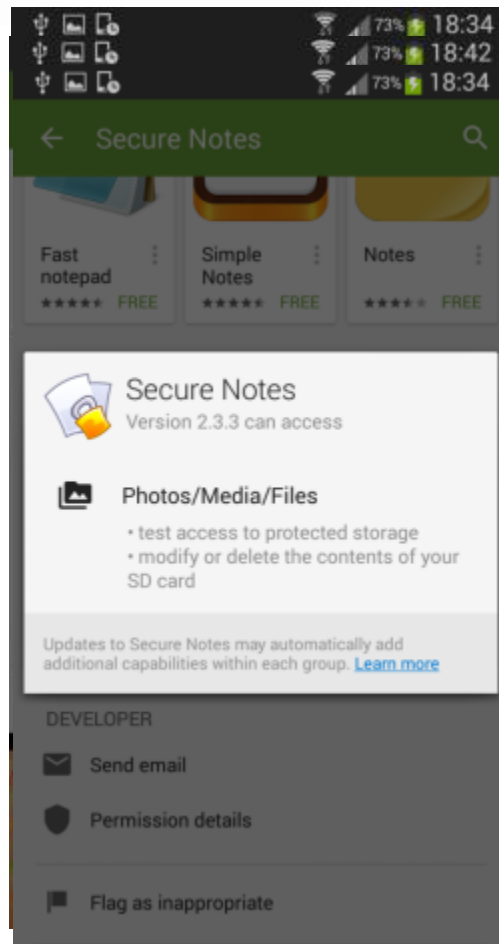
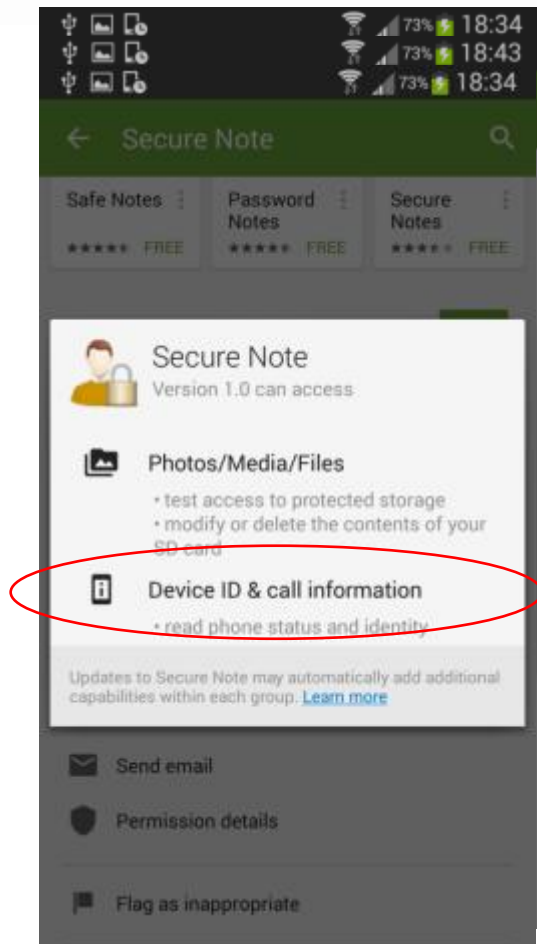
- 45% 沒有私隱政策聲明
- 85% 私隱政策聲明並不是就程式而編寫
- 8% 的程式開發商沒有提供足夠資料以確認其身份
- 6% 私隱政策聲明 不容易被閱讀

2013年5月

- 40%沒有私隱政策聲明
- 92%私隱政策聲明並不是就程式而編寫
- 60%的程式開發商沒有提供聯絡資料
- 11% 以 в другом языке 或 不容易被閱讀



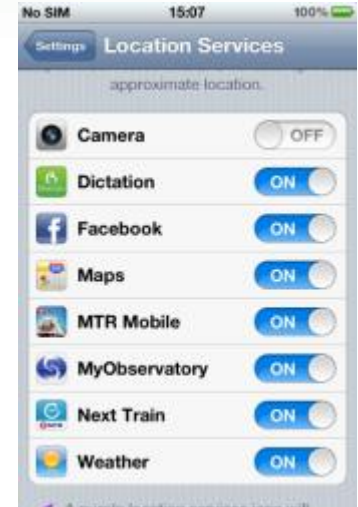
如何自保 - 明智選擇程式





保障私隱 – 明智使用程式

- 一張圖片勝過千言萬語
 1. 關閉相片的地理標記
 2. 關閉位置服務及移除過往的地理標記紀錄
 3. 定期查閱位置服務允許權
 4. Whatsapp 中應使用沒意義的個人圖像





網上私隱要自保

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

保障個人資料 • 互聯網 • 智能手機 • 社交網絡 • 公司機構 • 資源 • 公署活動 • 私隱政策聲明

網上私隱要自保
Think PRIVACY Be SMART Online

由香港個人資料私隱專員策動的網上私隱要自保專題網站，為你提供一站式的資訊和貼士，助你保護電腦和互聯網上的個人資料，減低網上私隱受侵犯的風險。

“精明使用手機應用程式”短片

<http://www.pcpd.org.hk/besmartonline/>



開發者需知





私隱及流動應用程式的開發

請參閱“流動應用程式開發商及其委託人須知”資料單張

http://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/apps_developers_c.pdf



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

資料單張

保障個人資料私隱：流動應用程式開發商及其委託人須知

引言

本技術資料單張旨在重點指出流動應用程式開發商（包括委託他人開發流動應用程式的機構）及營運商（在本單張統稱為應用程式開發商）在設計及開發流動應用程式前應考慮該等程式對私隱的影響。當中建議了一些符合《個人資料（私隱）條例》（下稱「條例」）（特別是其六項保障資料原則¹）的保障私隱行事方式，以供應用程式開發商跟從。

何謂流動應用程式？

就本單張而言，流動應用程式指可以捕捉流動裝置的位置資訊、查閱通訊錄、

一般而言，應用程式開發商會直接向流動裝置使用者收集其個人資料。此外，應用程式開發商亦可能在有或沒有通知流動裝置使用者的情況下透過流動應用程式查閱、轉送、分享或上載流動裝置使用者提供或流動裝置內之資料。至於流動應用程式所收集的資訊是否構成個人資料及受條例所管轄，則必須按每個個案的個別情況來判斷。任何資料若全部符合下述三個條件，則可被視為個人資料：

(a) 直接或間接與一名在世的個人有關的；



私隱及透明度

請參閱“擬備收集個人資料聲明及私隱政策聲明指引”

http://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/GN_picspps_c.pdf



引言

本指引旨在為資料使用者在擬備《收集個人資料聲明》及《私隱政策聲明》方面提供參考。《收集個人資料聲明》及《私隱政策聲明》分別是資料使用者依從《個人資料(私隱)條例》(「條例」)保障資料第1(3)原則(「第1(3)原則」)及第5原則(「第5原則」)規定的重要工具。

法律規定

第1(3)原則規定，資料使用者在直接向資料當事人收集個人資料時，須採取所有合理地切實可行的步驟，以確保：

- (a) 在收集資料當事人的個人資料之時或之前，以明確或暗示方式告知資料當事人，他是

甚麼是個人資料？

根據條例，「個人資料」指符合以下說明的任何資料：

- (a) 直接或間接與一名在世的個人有關的；
- (b) 從該資料直接或間接地確定有關的個人的身份是切實可行的；及
- (c) 該資料的存在形式令予以查閱及處理均是切實可行的。

資料使用者經常會特意地收集或查閱各類人士的個人資料，並有意或試圖確定這些人士的身份。在某些情況下，其收集的資料總結起來而可能已經足以識別出個別人士的身份。例如，一間公司追蹤記錄顧客對其產品或服務的消費



開發流動應用程式最佳行事方式指引

請參閱“開發流動應用程式最佳行事方式指引”

http://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/Mobileapp_guide_c.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



開發流動應用程式最佳行事方式指引： 單元及流程表

何時閱覽 WHEN TO READ

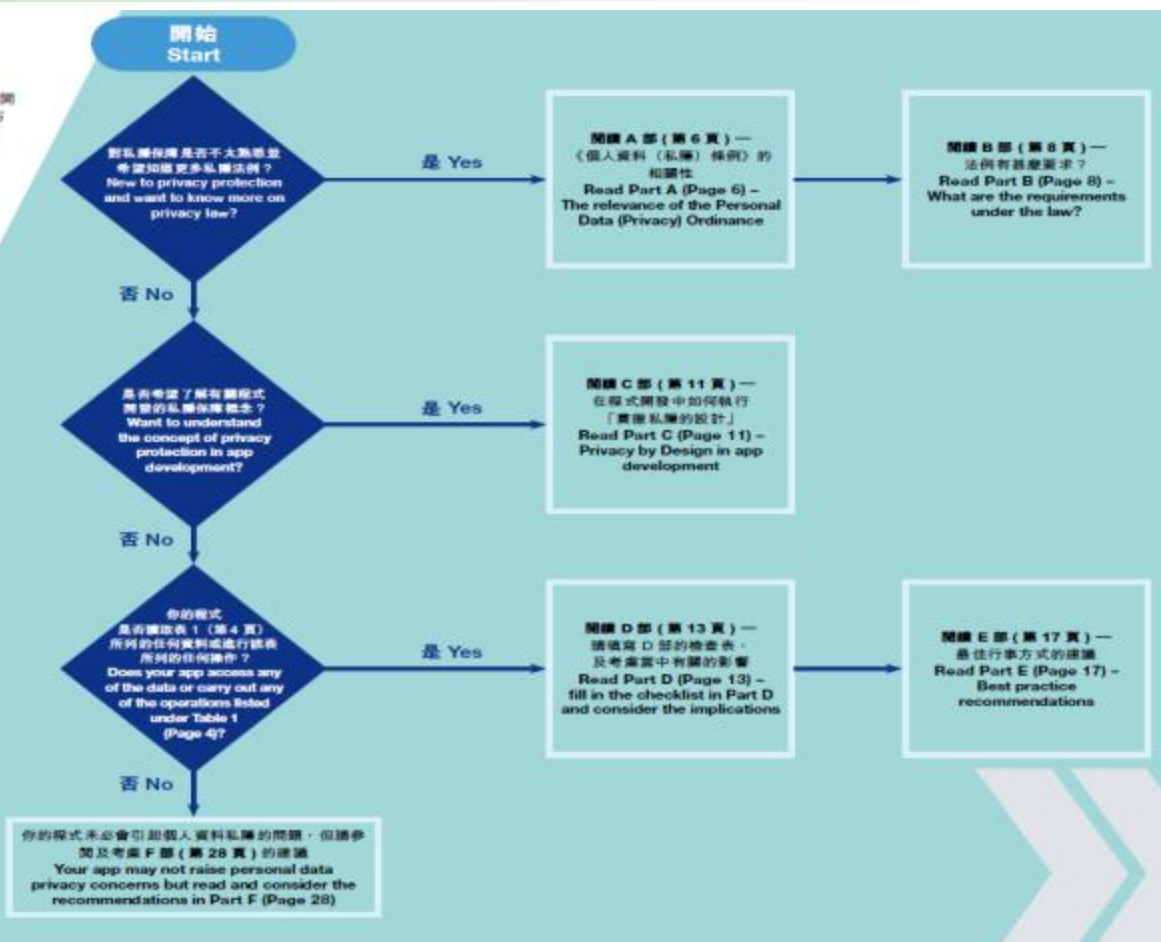
你應在開始計劃開發程式時便閱覽本指引。對企業來說，在開始階段便融入保障私隱的概念，相比日後為符應才作出這方面的調整，前者的花費會較少，而其對程式功能的影響也較為輕微。

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：

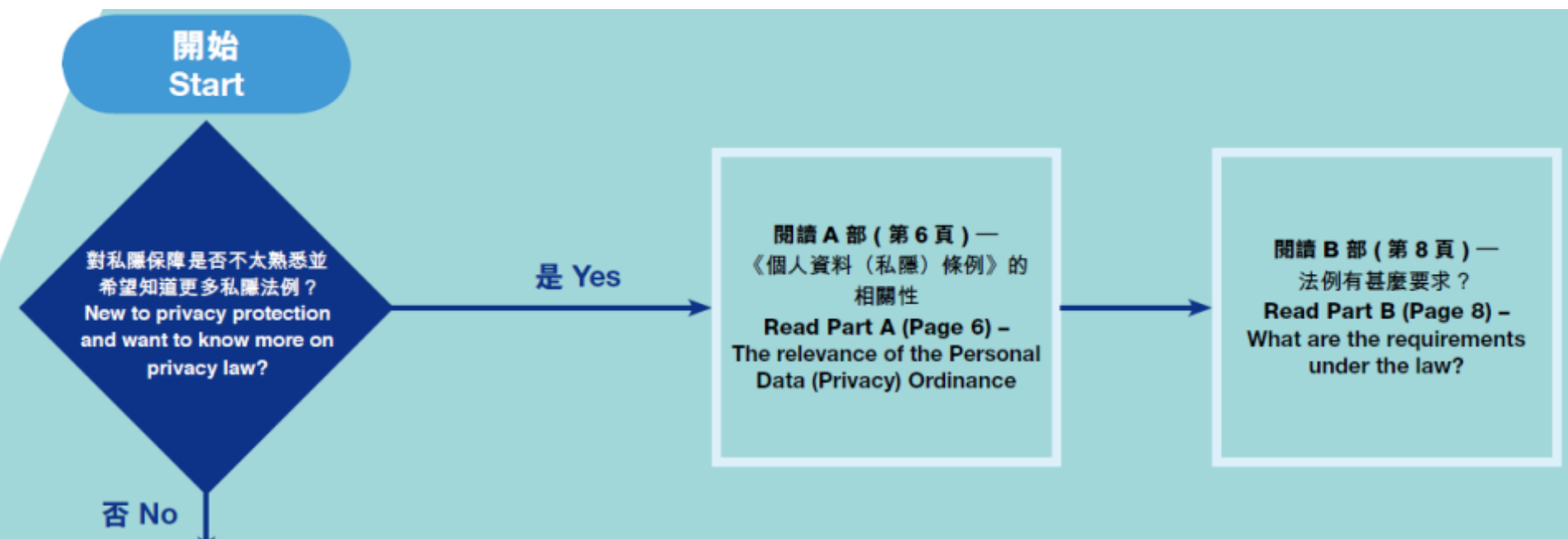
This guide comprises a number of parts which may be read independently. The flow chart on the right suggests how this guide may be used.



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



開發流動應用程式最佳行事方式指引： 法例要求





開發流動應用程式最佳行事方式指引： 「貫徹私隱的設計」說明

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

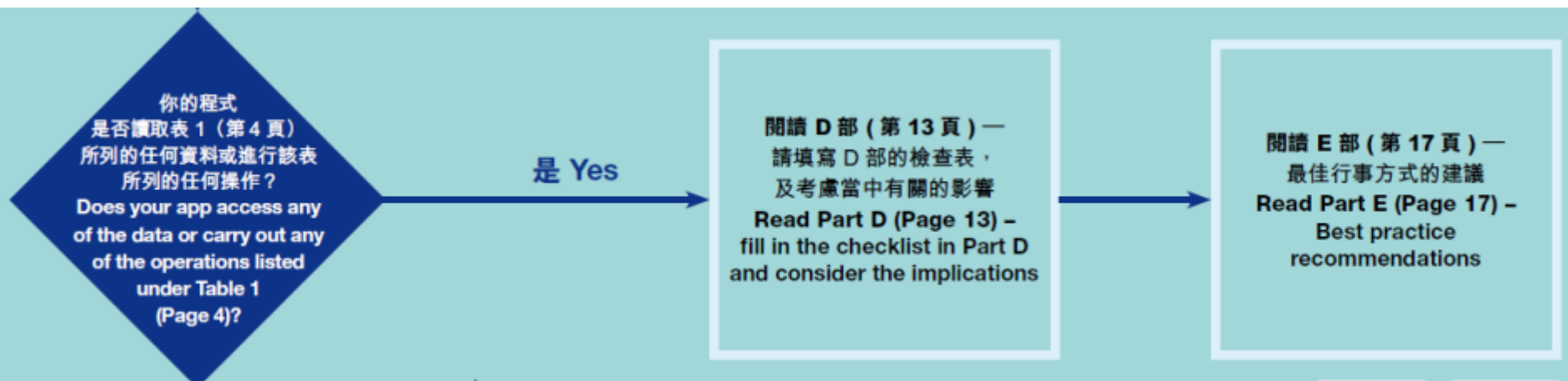
是 Yes

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

否 No



開發流動應用程式最佳行事方式指引： 最佳行事方式的建議





開發流動應用程式最佳行事方式指引： 自我評估檢查表

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 用戶登入 Require/allow user login	獲取 其他資料 Obtain other info
1. 是否絕對需要獲取 / 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方工具 (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													



開發流動應用程式最佳行事方式指引： 透明度





失誤抑或不在乎？

新聞稿



HKA HOLIDAYS

香港航空旅遊

日期：2014年12月15日

香港航空旅遊有限公司不慎使用流動應用程式「俠客行·旅行」外洩個人資料

(2014年12月15日) 個人資料私隱專員公署(「公署」)今日發表一份調查報告，指香港航空旅遊有限公司(「港航旅遊」)於iOS平台運行的流動應用程式「俠客行·旅行」(「俠客行」)外洩顧客的個人資料，原因是其程式保養承辦商佰邦達科技(北京)有限公司(「佰邦達」)沒有就iOS7推出新增保障私隱的功能(阻止程式讀取MAC位址¹作為識別流動裝置)，及時作出相應行動。而作為資料使用者的港航旅遊，違反了《個人資料(私隱)條例》(「條例」)附表一保障資料第4(1)原則。

背景



Android的權限缺陷



日期：2014年12月15日

私隱專員發現Android的權限模式有缺陷

(2014年12月15日) 個人資料私隱專員公署(「公署」)發現Android程式可以被編寫至在未有作出權限聲明的情況下，讀取Android 4.3或之前版本的流動裝置的公共記憶體。

2. Android一直以來的運作模式是，程式要讀取的資料會在安裝程式前呈現在「權限」頁面¹，若沒有呈現即不能被讀取。然而，公署的測試揭示，程式有機會在毋須於權限頁面作有關聲明的情況下，仍可讀取Android裝置內的記憶體內容，包括相片、檔案及其他程式儲存在該記憶體的資料。雖然有關可以讀取公共記憶體的缺陷已在Android 4.4的裝置糾正，但可以讀取部分內部記憶體的情況仍有可能於Android 4.4發生，故此情況依然值得關注。再者，目前有三分之二的Android用戶仍在使用Android 4.3或更舊的版本²，當中部份裝置更無法更新至Android 4.4。



Android的權限缺陷

Android 程式並非需要就每項讀取權限都通知用家：

裝置上的Android版本	權限頁面有否顯示任何權限？	可否讀取公共記憶體？	可否讀取部分內部記憶體？
Android 4.3 or 之前	x	✓	✓
Android 4.4	x	x	✓

程式需利用加密以保護其儲存於記憶體的資料



問答時間

