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、行事曆或相片簿，及/或經互聯網或流動電話網絡支援語音/多媒體通訊的流動裝置應用程式。這類裝置一般包括智能電話及平板電腦。

流動應用程式、個人資料與條例

因為流動裝置經常會被當作私人記事本及隨身攜帶，因此它們一般被視為非常個人及私人的物品。這些流動裝置儲存的資料包括行蹤位置、拍攝的相片、發送及收取的短訊、輸入的聯絡資料，以及使用的社交網站用戶名稱和密碼。

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；
(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。

私隱風險

應用程式開發商應注意，當集結其廣泛收集或存取之資料後，或可從中辨識個別人士。此外，隨着所收集得來之個人資料與日俱增，應用程式開發商因而可建立個別人士之活動概覽，引申令人關注的私隱問題。

[1] 請參閱：
http://www.pcpd.org.hk/chinese/ordinance/ordglance.html

鼓勵採用的良好行事方式

有鑑於此，雖然條例下沒有特別規定，但公署鼓勵應用程式開發商採取下述的良好行事方式來保障個人資料：

保障私隱　全面貫徹

在設計流動應用程式時，如開發商擬在流動裝置查閱/分享個人資料的應用程式，應採取「保障私隱　全面貫徹」的理念（即從開始設計便納入保障私隱的理念）。這個理念有七項原則：

1. 個人資料保障應是主動（而並非被動）及預防性（而並非補救性）的；
2. 個人資料保障應是預設的設定；
3. 個人資料保障應納入在流動應用程式的設計之中，而不是待設計後才額外裝置的；
4. 應用程式的功能或保安上的設計應與個人資料私隱設計的考慮互相補足，而不是因此有所犧牲；
5. 個人資料保障應涵蓋由收集以至刪除個人資料的整個流程；
6. 個人資料私隱設計的考慮應公開予持份者及具透明度；
7. 個人資料私隱設計的考慮應以用者為本。

私隱影響評估

私隱影響評估是「保障私隱　全面貫徹」的工具，能有系統地於早期評估一個程序或系統（例如流動應用程式）的設計對個人資料私隱的影響，目的在於檢測風險及避免或減低任何不利的影響。雖然條例沒有明確規定資料使用者需要進行私隱影響評估，但公署鼓勵應用程式開發商在設計及開發流動應用程式前，採用這種已眾所周知的循規及風險評估工具。

有關詳情，請參閱個人資料私隱專員（下稱「**專員**」）發出的《私隱影響評估》資料單張[2]。

遵從保障資料原則的建議行事方式

應用程式開發商如透過流動應用程式收集個人資料，必須遵守條例的規定，包括其中監管收集、持有、處理及使用個人資料的機構（在條例稱為「**資料使用者**」）的六項保障資料原則。以下為該六項保障資料原則及建議應用程式開發商遵從的良好行事方式。

保障資料第 1 原則 – 收集的目的及方式

- 從/經流動裝置收集或傳輸個人資料的目的必須屬合法及與資料使用者的職能或活動直接有關；
- 所收集的個人資料必須屬足夠但不超乎適度；
- 個人資料必須以合法及公平的方式收集；
- 如個人資料是直接從個人（在條例稱為「**資料當事人**」）收集，資料當事人應獲告知他有責任提供或可自願提供該資料、收集資料的目的、該資料可能移轉予甚麼類別的人，以及要求查閱及改正該資料的權利。這些資料一般會列於收集個人資料聲明中。

[2] 請參閱：
http://www.pcpd.org.hk/chinese/publications/files/PIAleaflet_c.pdf

收集個人資料聲明

應用程式開發商須在收集流動裝置使用者之個人資料之時或之前提供收集個人資料聲明，告知流動裝置使用者其個人資料會在甚麼情況下被收集、查閱或分享，及作何等用途。這通知應在流動裝置使用者確認流動應用程式的安裝前清楚向其呈示。

流動應用程式聲明

如查閱某資料的權限需要在流動應用程式的編程代碼中聲明，流動裝置才會授予，應用程式開發商應確保有關查閱確實是在流動應用程式內作出。如流動應用程式的查閱權限聲明所涵蓋的資料多於流動應用程式所需使用的，一旦流動裝置使用者察覺到已作出聲明的查閱屬不必要/沒有被使用，便會引起他們對該流動應用程式的意圖及真實性的懷疑。舉例說，如流動裝置使用者在一個動作遊戲的權限頁中得悉該遊戲會查閱其流動裝置內的日記，那麼儘管這遊戲從沒有查閱任何日誌，流動裝置使用者亦會質疑這個需要，並或會停止使用這遊戲。

權限模式

對於流動裝置使用者來說儲存在流動裝置內的資訊多屬敏感資料，在公平的原則下，應用程式開發商應全面通知流動裝置使用者有關其資料之收集、轉發或分享。此外，公署亦鼓勵應用程式開發商考慮採用以權限為基礎的查閱模式，即每當首次查閱、轉發或分享每項新類型資訊時，須徵得流動裝置使用者允許。此為確保流動裝置使用者知悉每項資料查閱、轉發或分享的進行。流動應用程式亦應允許流動裝置使用者選擇個別資料發放權。此外，應用程式開發商應考慮在流動應用程式設立設定畫面，顯示流動裝置使用者對每類資訊所給予的允許權限，並容許流動裝置使用者其後更改/取消個別之查閱權限。

保障資料第 2 原則 – 準確性及保留期間

- 資料使用者必須採取所有切實可行的步驟以確保所持有的個人資料的準確性；
- 資料使用者必須採取所有切實可行的步驟以確保所保存的個人資料不會超過該資料被使用於的目的所需的時間；
- 如資料使用者聘用資料處理者[3]以代其處理個人資料，該資料使用者須採取合約規範或其他方法，以防止轉移予該資料處理者的個人資料的保存時間超過處理該資料所需的時間。

不必要地保留個人資料

根據上述保留原則，應用程式開發商須於流動應用程式不再需要某資訊時，盡快將已上載或儲存於後端伺服器的相關資訊完全棄置。舉例說，如流動應用程式在每次運作前，必須先把通訊錄的最新複本上載至伺服器，則舊有已上載的複本應當在完成其功能後獲刪除。

[3] 資料處理者指代另一人處理個人資料；及不為該人本身目的而處理該資料的人。

移除承諾

應用程式開發商在收到流動裝置使用者要求或帳戶終止後，除非基於法律或監管原因，否則應徹底移除帳戶資料（包括已上載或分享的資料）。應用程式開發商應確保這項帳戶移除功能易於取用。

外判

如應用程式開發商聘用外判代理代其開發或營運流動應用程式，他們應採用合約規範或其他方法要求外判代理：(i)保留查閱及使用個人資料的記錄；(ii)在指定情況及期限刪除個人資料；(iii)使用業界標準的資料刪除軟件；(iv)就刪除行動作出適時報告；及(v)容許由應用程式開發商或獨立人士檢視及審核。

有關詳情，請參閱專員發出的《外判個人資料的處理予資料處理者》資料單張[4]。

保障資料第 3 原則 －
個人資料的使用

- 如沒有資料當事人的訂明同意，其個人資料不得用於收集資料當時所提述的目的或有關目的以外的其他用途。

避免改變用途

應用程式開發商往往從流動應用程式收集個人資料及建立數據庫後，始發覺這些個人資料的其他潛在用途（例如數據開採、分析等）。如資料的新使用目的與原本收集目的並非直接有關，應用程式開發商在使用前必須取得流動裝置使用者明確及自願的同意。

保障資料第 4 原則 －
個人資料的保安

- 資料使用者必須採取合理地切實可行的步驟，以保障所收集的資料不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響。
- 如資料使用者聘用資料處理者，以代其處理個人資料，該資料使用者須採取合約規範方法或其他方法，以防止轉移予該資料處理者作處理的個人資料未獲准許或意外地被查閱、處理、刪除、喪失或使用。

軟件開發工具

如使用欺詐的軟件開發工具，可能會不知情地引入一些不需授權便可查閱流動裝置資料的木馬或後門程式。為避免以上情況發生，應用程式開發商在開發流動應用程式時應使用可靠及/或官方版本的軟件開發工具（例如軟件開發套裝、軟件庫）。

安全編碼

為減低被黑客入侵或因疏忽而造成的資料外洩，應用程式開發商亦應依從業界就安全編碼的最佳行事方式來編寫程式，以確保其流動應用程式安穩健全。特定電腦語言的安全編碼指引可從例如 CERT[5] 等機構取得。此外，個別流動裝置製造商亦會自行編製安全編碼指引，應用程式開發商應在設計及開發流動應用程式時參考這些指引。

[4] 請參閱：
http://www.pcpd.org.hk/chinese/publications/files/dataprocessors_c.pdf

[5] 請參閱：http://www.cert.org/secure-coding/ （只提供英文版）

加密

所有流動應用程式傳輸的資訊應該受到加密保護，以防被截取。如資訊必須儲存於後端伺服器，儲存的資訊應以存取監控及加密方式保護，以免受到未經准許的查閱。

代碼審查及測試

應用程式開發商在正式推出流動應用程式前，應進行代碼審查及測試，這樣不單是要找出漏洞，亦為了確保流動應用程式並無設計規格以外資料查閱的功能（不論是有意或無意的）。

外判

如應用程式開發商聘用外判代理代其開發或營運流動應用程式，他們應採用合約規範或其他方式要求外判代理(i)使用正版（即非盜版）及可靠的開發工具及軟件；(ii)對其職員就個人資料的存取有正規的監控；(iii)迅速滙報任何資料外洩事故；(iv)容許由應用程式開發商或獨立人士檢視或審核；及(v)除非可以保證有相同水平的保護措施，否則不得把工作再分判或再外判。

有關這方面的更多資訊，請參閱上文提及的《外判個人資料的處理予資料處理者》資料單張。

保障資料第 5 原則 －
資訊須在一般情況下可提供

- 資料使用者必須切實可行地提供予任何人其個人資料私隱的政策及實務，包括其持有個人資料的種類及資料的使用目的。

私隱政策聲明

應用程式開發商應擬備私隱政策聲明，列明其在個人資料私隱保障方面的政策及實務。這份聲明應以容易閱讀及理解的方式呈示，避免使用一些技術性術語或難明的詞彙。此聲明在流動應用程式中應易於查找，亦應在應用程式開發商之網頁內予以提供。

在私隱政策聲明中提供例子

在描述資料的使用目的時，應用程式開發商應考慮提供針對有關流動應用程式的實例（而不是一般說明），以協助流動裝置使用者了解為何有關資料需要被收集、查閱或分享。

相關性及準確性

應用程式開發商應確保其私隱政策聲明乃針對該特定流動應用程式而提供具體及準確的描述。如聲明過於含糊不清，應用程式開發商可能會被視作對該流動應用程式收集及查閱資料的目的有所隱瞞。同樣地，如私隱政策聲明乃複印或摘錄自標準模板或另一流動應用程式，應用程式開發商必須檢討其內容，以確保其相關性及準確性。

保障資料第 6 原則 －
查閱個人資料

- 資料當事人有權要求資料使用者確定是否持有其個人資料，及要求索取所持有個人資料的複本。資料當事人亦有權要求改正有關資料。

提出查閱及改正資料要求的聯絡資料

應用程式開發商應於流動應用程式中提供聯絡資料（包括姓名或職銜及地址），讓流動裝置使用者就查閱及改正其個人資料提出要求。應用程式開發商亦應確保他們有相關政策及程序以配合有關要求必須在條例所定的 40 日時限內獲處理。請參閱專員發出的《資料使用者如何妥善處理查閱資料要求及收取查閱資料要求費用》[6]。

應用程式開發商負責遵從條例規定

上述建議或鼓勵採用的措施並非包羅無遺，亦不表示它們可以製造出完全合乎法例的流動應用程式。應用程式開發商須就不同流動應用程式之特點及功能，小心謹慎地找出最適合依從條例規定的方法來保障個人資料。

香港個人資料私隱專員公署
查詢熱線： (852) 2827 2827
傳真： (852) 2877 7026
地址：香港灣仔皇后大道東 248 號 12 樓
網址：www.pcpd.org.hk
電郵：enquiry@pcpd.org.hk

[6] 請參閱：
http://www.pcpd.org.hk/chinese/publications/files/DAR_c.pdf