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

2014 年智能手機應用程式抽查報告：
私隱政策透明度

2014 年 12 月

目錄

引言

2013 年 5 月，個人資料私隱專員公署（「公署」）作為「全球私隱執法機關組織」「2013 互聯網私隱風險搜尋」聯合行動[1]的一份子，就流動應用程式（「程式」）的私隱政策透明度進行了研究。

2. 當時公署抽查了 60 個由本港開發的最熱門智能手機程式，結果顯示它們的私隱政策透明度普遍不足，僅六成程式備有《私隱政策聲明》，絕大部分都沒有提供充足的資訊解釋程式讀取手機上哪些資料以及其目的。公署其後於 2013 年 8 月 14 日發表了有關的抽查報告[2]。

3. 在 2013 年聯合行動中，公署是兩個對程式進行研究的私隱執法機構之一，而其餘 17 個機構則研究網站的私隱政策透明度。

4. 由於近幾年程式激增且非常普及，26 個本年參與 2014 年聯合行動[3]的私隱執法機構決定專注於研究程式的私隱政策透明度。

主旨

5. 2014 年聯合行動旨在提升公眾及商界對私隱權利及責任的意識；了解需要處理的私隱關注；以及推動機構遵從私隱法例。特別在程式方面：

5.1 是次研究調查程式（或程式開發商）如何向顧客解釋其讀取／收集資料的原因及會如何處理資料；及

5.2 是次研究亦會檢視程式尋求的權限種類，相對於程式表面上的功能而言，是否超乎用家的預期。

---

[1]「全球私隱執法機關網絡」的「2013 年互聯網私隱風險搜尋」聯合行動（「2013 年聯合行動」），旨在評估機構資料使用者在收集及使用網上個人資料方面的公開和透明度（請參閱公署於 2013 年 5 月 7 日發出的新聞稿：www.pcpd.org.hk/chinese/infocentre/press_20130507.htm）。包括公署在內的 19 個私隱執法機構參與這個聯合行動，以提升公眾及商界對私隱權利及責任的意識；了解需要處理的私隱關注；以及推動機構遵從私隱法例。各地私隱執法機構在聯合行動中自行選擇其研究範圍和重點。公署選擇了研究智能手機程式在交代其私隱政策方面的透明度。

[2]《智能手機應用程式抽查報告：私隱政策透明度》（www.pcpd.org.hk/chinese/publications/files/mobile_app_sweep_c.pdf）

[3]「全球私隱執法機關網絡」的「2014 年私隱風險搜尋」聯合行動（「2014 年聯合行動」），旨在評估機構資料使用者在流動應用程式的個人資料收集及使用。包括公署在內的 26 個私隱執法機構參與 2014 年聯合行動，以提升公眾及商界對私隱權利及責任的意識；了解需要處理的私隱關注；以及推動機構遵從私隱法例。

程式的甄選

6. 根據環球業內數字（包括公署於 2012 年年底發表的調查報告），使用中的智能電話大部分是採用 Google Android 或 Apple iOS （iPhone）的操作系統。因此，參與 2014 年聯合行動的所有私隱執法機構決定只研究 Android 及 iPhone 程式的私隱政策透明度。

7. 各私隱執法機構可根據其本地情況自行決定研究程式的數目及種類。香港方面，為了與 2013 年的程式抽查準則一致，公署從 Android 及 iOS 操作系統中各揀選了 30 個程式，並採用與去年同樣的準則從「熱門排行榜」中甄選程式，以追蹤本地開發程式的私隱透明度趨勢。有關準則為：

7.1 兩個操作系統的官方程式商店（即 Android 的 Google Play Store 及 iPhone 的 App Store）各自提供的三個「熱門排行榜」（即「熱門免費項目」、「熱門收費項目」及「最賣座項目」[4]）中最流行的程式；

7.2 程式須由在香港有實體運作的開發商開發；及

7.3 程式聲稱會讀取以下一項或多於一項儲存於裝置或可於裝置讀取的私人資料：

7.3.1. 手機獨特識別碼（IMEI 碼）；
7.3.2. 手機定位位置資料；
7.3.3. 儲存在手機上的帳戶資料；
7.3.4. 手機內儲存或將接收的 SMS 訊息；
7.3.5. 鏡頭及／或錄音功能；
7.3.6. 通話紀錄；
7.3.7. 通訊錄／聯絡資料；
7.3.8. 行事曆資料；
7.3.9. 內部記憶；及
7.3.10. 手機正在執行的程式。

8. 程式的甄選於 2014 年 5 月 12 日（即 2014 年聯合行動商定的開展日）進行。公署檢視該日兩個操作系統的三個「熱門排行榜」，以篩選出符合甄選準則的程式。公署原本計劃從每個「熱門排行榜」各選出 10 個程式，但符合所有甄選準則的程式中，收費的遠比免費的少。即使在詳細檢視「熱門收費」排行榜的所有程式後，亦無法從任何一個操作系統中選出 10 個符合甄選準則的收費

[4] 程式市場中的「熱門免費項目」、「熱門收費項目」及「最賣座項目」排行榜分別呈列最受歡迎的免費、收費及賣座程式。這些排行榜會經常更新，以反映不同國家及地區的趨勢。

程式。因此，是次抽查樣本最終從兩個操作系統分別甄選 30 個本地開發程式，但相對地在 App Store 中甄選了較多「熱門免費」程式及「最賣座」程式，而在 Google Play Store 中則甄選了較多「熱門免費」程式。

9. 合共抽查的 60 個程式是由 45 個資料使用者開發。程式分佈如下：

操作系統	熱門免費	熱門收費	最賣座	總數
Android	24	1	5	30
iPhone	14	2	14	30

10. 2014 年抽查行動中被甄選以作研究的全部程式名單詳見附錄 A。該等程式分別被安裝於 Android 4.3 及 iOS7 版本的智能手機以作檢視。

11. 由於 Android 在安裝過程中會透過呈示的「權限」頁[5]告訴用家其讀取的資料種類，而 iPhone 程式則不能，故甄選過程作出了以下一個假設：同一款程式，在兩個操作系統的版本所讀取的資料類別會是相同的。由於相對 Android 程式而言，iPhone 程式沒有提供相同程度的透明度[6]，所以要判斷 iPhone 程式有否讀取手機某項資料，便要依靠檢視相應的 Android 版程式作決定。

檢視方式

12. 2014 年抽查行動不為程式的設計及開發作出深入分析，而是就一套指標檢視安裝及使用程式的體驗。

13. 公署就每個經甄選的程式檢視了下述範疇：

13.1 程式有否在程式市場中提供《私隱政策聲明》（或同等資訊）？

13.2 若程式沒有在程式市場中提供《私隱政策聲明》，開發商的網站有否提供私隱政策？

13.3 《私隱政策聲明》有否具體及充分地就程式讀取／收集／使用及／或披露私人資料的情況提供資訊？

[5]在安裝Android程式時，Android用家會看到一個「權限」頁，列出該程式能夠讀取Android裝置內所儲存的資料類別。就此，用家可以選擇繼續或終止安裝（但不能個別地選擇容許該程式讀取哪些類別的資料）。基於Android程式的技術架構，程式不能讀取這權限頁中沒有「申報」的資料類別。

[6] iPhone 程式在安裝之前或之時不會向用家列明會讀取的資料類別。不過，對於 iOS7（本研究進行時 iPhone 操作系統通行的版本）用家，在某程式運行時及首次讀取某類資料（即相片集、通訊錄、日誌、提示、位置資料及使用麥克風時）之前，該程式會要求用家給予它讀取該類資料的權限。用家有權容許或拒絕該程式讀取該類資料，而該程式應按用家指示而行。

13.4 程式是否具有內置廣告？

13.5 程式是否需要（強制性）或支援（可選擇的）用家登入？如有，是否必須為此開設新帳戶或使用已開立的第三者帳戶（如 Google、Facebook 等），或兩者皆可？

14. 每個程式被檢視的項目詳列於附錄 B。由於部分問題需要進行評估的人員（抽查者）的主觀判斷，因此每個程式均由公署兩名人員評估，而他們都是具有關操作系統經驗的用家。兩名人員對每個程式的判斷結果會由第三名人員匯集，如當中有巨大差異，第三名人員會作出調整。這項安排旨在取得可代表典型智能電話用家的體驗的結果。

15. 本報告以下部分列出各項結果。檢視後並無重要發現的項目將不會被提及。

抽查結果

16. 在討論抽查結果之前，應留意程式市場的發展瞬息萬變，因此，本報告的結果只能反映香港的程式在某特定時間的一般私隱政策透明度。

17. 是項行動只屬一般抽查，而非正式的審查或調查。由於公署沒有對每個被抽查的程式投放同等循規行動或調查的資源，及沒有向各開發商作出正式查詢，現階段不適宜透露個別程式的負面抽查結果。

呈示的抽查結果類別

18. 2014 年抽查行動的結果分為兩類：**概括結果**及**特定結果**。

19. **概括結果**是從檢查所有程式所得出的整體趨勢及觀察。概括結果分三類呈示：

19.1. **逐年指標**（提供聲明、容易找到、聯絡資料、可讀性及相關性）是以類似去年的方式搜集的指標。這些指標會與去年數字作比較；

19.2. **2014 年指標**為只限於今年香港抽查研究所收集的指標，以進一步探討程式行為；及

19.3. **2014 年環球指標**是所有參與 2014 年聯合行動的私隱執法機構同意收集的主要指標。香港得出的結果會與環球結果作比較。在此必須再強調，這些指標大多需由抽查人員自行判斷（例如程式有否充分

解釋其權限要求），但為對準要求，公署已透過評估表格提供例子及指引（例如，若所有權限都備有解釋，答案即為「是」；若只有部分權限有解釋，答案即為「不足」）。

20. 對個人資料私隱保障有重大影響的**特定結果**如下：

20.1. **權限**—我們評估程式可讀取的資料類別時，發現很多資料類別有可能被用作追蹤程式用家的行為及喜好。因此我們認為程式開發商能清楚解釋為何其程式需要讀取這些資料，及資料會如何被進一步使用等是非常重要的；及

20.2. **記憶讀取**—我們發現能夠於 Android 智能電話中讀取分享記憶的程式，在安裝時無需呈示任何權限要求。這個現象已經由公署自行開發的一個 Android 程式所確定。這做法容許程式在無需告知用家的情況下無限制地讀取電話內的分享記憶，屬需關注事項。

21. 在 2014 年抽查行動中，我們發現「我的天文台」程式提供非常清晰的《私隱政策聲明》及採用具私隱保護的設計，特此表揚程式開發商的努力。

概括結果—逐年指標

22. **提供聲明**：《私隱政策聲明》是否可以在安裝程式前或在開發商的網站找到：

	2014 年抽查行動 (總共 60 個程式)	***2013 年抽查行動 (總共 60 個程式)***
在安裝程式前找到《私隱政策聲明》[7]	15 (25%)	*0 (0%)*
在開發商的網站找到《私隱政策聲明》[8]	18 (30%)	*36 (60%)*
找不到《私隱政策聲明》[9]	27 (45%)	*24 (40%)*

23. **容易找到**：《私隱政策聲明》是否清楚呈示於網站的「私隱政策」一欄下：

[7]「在安裝程式前找到《私隱政策聲明》」是指在程式市場內透過連至開發商網站的連結（標示為「私隱政策」）找到《私隱政策聲明》。

[8]「在開發商的網站找到《私隱政策聲明》」是指在程式的安裝前沒有於螢幕上呈示「私隱政策」。抽查者可能在安裝程式前取得開發商的網址或猜測網址。

[9]對比之下，2014 年環球抽查中 991 個應該提供《私隱政策聲明》的程式中，有 300 個（30%）找不到《私隱政策聲明》。

	2014 年抽查行動 (總共 33 個程式)	***2013 年抽查行動 (總共 36 個程式)***
網站的「私隱政策」一欄找不到《私隱政策聲明》[10]	4 (12%)	*7 (19%)*[11]

24. **聯絡資料**：程式在安裝前有否提供任何聯絡資料（例如網站、電話號碼、電郵地址、傳真號碼及／或地址）：

	2014 年抽查行動 (總共 60 個程式)	***2013 年抽查行動 (總共 60 個程式)***
提供最少一項聯絡資料（例如電郵，電話，地址等）	60[12] (100%)	*36 (60%)*

25. **可讀性**：《私隱政策聲明》是否容易閱讀：

	2014 年抽查行動 (總共 33 個程式)	***2013 年抽查行動 (總共 36 個程式)***
《私隱政策聲明》難以閱讀	2 (6%)[13]	*4 (11%)*[14]

26. **相關性**：向程式用家呈示的《私隱政策聲明》是否針對該程式或屬一般性：

	2014 年抽查行動 (總共 33 個程式)	***2013 年抽查行動 (總共 36 個程式)***
在安裝程式前向用家提供針對該程式的《私隱政策聲明》	2 (6%)	*1 (3%)*
在安裝程式後向用家提供針對該程式的《私隱政策聲明》	3 (9%)	*2 (6%)*

[10] 《私隱政策聲明》被放置於其他連結項目內，例如公司資料、條款及細則、客戶專區或會員專區。
[11] 在 2013 年抽查行動中，《私隱政策聲明》被放置於其他連結項目內，例如服務條款、登記成為互動會員、客戶服務或重要告示。
[12] 有 5 位開發商的身份從提供的聯絡資料中仍然不能直接地被確立。
[13] 在兩個程式中，合共 126 行的《私隱政策聲明》是在開發商的網站以小框格、每次八行的形式提供。
[14] 在 2013 年抽查行動中，有兩個程式只提供英文版聲明（但程式以中文編寫），另外兩個開發商合共 292 行的聲明則在網站以小框格、每次八行的形式提供。

27. **比較去年，觀察結果如下：**

27.1. 相比去年的 40%，今年沒有提供任何《私隱政策聲明》的程式數目仍然高企於 45%；

27.2. 在安裝程式前提供聯絡資料（網站連結及／或電郵地址）的程式數目有改善，由去年的 60%上升至今年的 100%；及

27.3. 本年的部分程式開發商的身份不能被確定。即使在安裝時程式有提供網站連結及電郵地址，但至少五個程式（8%）的開發商身份最終不能被確定[15]。

概括結果—2014 年指標

28. **刊登廣告的程式**：60 個程式中，35 個（58%）有展示廣告，當中 23 個（38%）展示第三者提供的廣告。

29. **要求登入的程式**：60 個程式中，30 個（50%）要求（容許）用家在使用時以帳戶登入。在這 30 個程式中，15 個（25%）容許用家使用第三者（通常是社交網站）帳戶登入程式。

30. **從這些 2014 年指標所得的觀察如下：**

30.1. 程式開發商或廣告商有誘因在刊登的廣告中追蹤用家的行為及／或喜好。程式開發商或廣告商因此應該提供透明度，告知用家他們是否這樣追踪用家及用家能否拒絕被追蹤；

30.2. 有些需要用家登入使用的程式會容許用家透過其社交網站帳戶登入，而無需就該程式開設新帳戶。不過，程式開發商卻因而可以把用家的行為或身份與其社交網站帳戶的身份資料結合起來；及

30.3. 在容許程式用家使用社交網站帳戶登入的 30 個程式中，沒有一個表明會否把用家的社交網站帳戶與用家在程式中的行為資料結合。在 35 個會展示廣告的程式中，沒有一個表明會否追蹤用家與廣告之間的互動交流（例如用家有否開啟／觀看廣告及哪個廣告）。程式開發商應留意這些情況可能導致的私隱關注並在其《私隱政策聲明》中清楚說明其運作，向用家保證尊重其私隱。

[15] 在這五個程式中，兩個提供至社交網絡頁的連結，但沒有顯示開發商的身份。另外兩個提供至其網頁並有電郵地址的連結，但開發商的身份不能從網頁或電郵地址確定。最後一個提供至其網頁的連結，但沒有任何聯絡資料。

概括結果—就 2014 年共同指標比較本地與環球結果

31. **安裝前的溝通：**在安裝前沒有提供或提供不清晰的私隱告示／通訊（例如程式在下載前提供很少關於私隱措施的資訊、提供的連結並不存在、在提供連結的網頁／社交媒體網頁中沒有透露程式開發商的身份，或只提供不是為程式編寫的一般私隱政策）：

	香港 (總共 60 個程式)	***環球 (總共 1,211 個程式)***
不清晰或沒有解釋程式會否閱讀資料，會閱讀甚麼資料，及為何閱讀該資料	43 (72%)	*715 (59%)*

32. **細小螢幕：**沒有因應細小螢幕而制訂私隱訊息：

	香港 (總共 31 個程式)	***環球 (總共 1,211 個程式)***
沒有因應細小螢幕而制訂私隱訊息	13 (42%)	*524 (43%)*

33. **過度權限：**需要的權限超越程式的表面功能：

	香港 (總共 60 個程式)	***環球 (總共 908 個程式)***
相會程式俱備的權限超越程式的表面功能	51 (85%)	*281 (31%)*

34. **用家整體滿意程度：**就所需權限及程式如何收集、使用或披露資料所作的解釋程度：

	香港 **(總共 60 個程式)**	***環球*** ***(總共 991 個程式)***
沒有提供私隱資訊	27 (45%)	*300 (30%)*[16]
有私隱資訊，但與程式無關	10 (17%)	
私隱資訊不足以讓抽查者了解程式如何使用資料	11 (18%)	*242 (24%)*
只有部分權限有提供私隱資訊，抽查者因此不能完全明白程式需要某些權限的原因	10 (17%)	*304 (31%)*
有提供清晰的私隱資訊	2 (3%)	*145 (15%)*

35. **與環球結果比較後，得出下述觀察：**

35.1. 就私隱資訊沒有因應細小螢幕而設的程式比例而言，香港結果（42%）與環球（43%）的數字大致相近（見上文第 32 段），但在其他方面，本地數字遠較環球數字為差：

35.1.1. 沒有提供或提供不清晰的安裝前告示比例偏高—本地為 72%，環球為 59%（見上文第 31 段）；

35.1.2. 權限可能超乎適度的程式比例較高—本地為 85%，環球為 31%（見上文第 33 段）；及

35.1.3. 有提供清晰私隱資訊的程式比例較低—本地為 3%，環球為 15%（見上文第 34 段）。

<u>結果—權限</u>

36. 如 2013 年抽查行動所得結果，除了程式的《私隱政策聲明》透明度外，程式所要求的權限仍是主要焦點。Android 及 iOS 程式如何處理權限事宜已分別在註釋 5 及 6 闡釋。以 Android 程式而言，在程式讀取資料之前，開發商必須先「申報」程式擬讀取的資料類別，而這些資料類別會在安裝程式時於「權限」頁向手機用家展示。開發商有可能申報多項它可能讀取的資料類別，但最終該程式不一定會或需要讀取所有申報項目。不過，Android 作業系統會限制程式於讀取任何資料前先向手機用家申報及展示。

[16] 不是所有參與的機構都有將「沒有提供私隱資訊」及「有私隱資訊，但與程式無關」的數字分開，因此只提供合併的數字。

37. 至於 iOS，目前沒有機制規定在程式安裝之前或之時向 iOS 用家顯示程式擬讀取的資料類別。不過，對於 iOS 第 7 版（抽查進行時通行的版本）的手機用家，如某程式擬讀取定位位置、通訊錄、日誌、相片集、提示及／或使用麥克風時，他們會收到特定的螢幕提示[17]。用家可以隨時決定是否容許某程式讀取有關類別的資料。

38. Android操作系統會在智能手機用家安裝程式前於「權限」頁展示將會讀取哪些資料，透明度算比較高。可是，其「權限」頁只展示哪些資料會被讀取而沒有說明為何程式要讀取這些資料。再者，Android用家沒有權選取甚麼資料可以被程式讀取。只要Android用家安裝這些程式，即暗示准許該程式讀取程式開發商已聲明會讀取的所有資料。

39. iPhone平台則在控制上較優越，它容許手機用家逐項決定上述六項資料是否可被讀取。雖然如此，手機上還存有很多其他私人資料。由於iPhone並無如Android般展示程式將會讀取的資料類別，除上述六項資料外，對於有甚麼其他資料會被讀取，iPhone用家基本上仍是被蒙在鼓裏的。

40. 以下部分概述這60個程式會讀取手機上的私人資料類別的研究結果。正如前述，由於iPhone程式在設計上不會向用家披露會讀取手機上甚麼類別的資料，評估iPhone的程式時只能假設iPhone程式版本所讀取的資料類別與Android版本相近。

41. 這 60 個程式會讀取的資料類別差別很大。詳細分項表列如下：

2014 年抽查結果—讀取的私人資料類別數量：

讀取的私人資料類別的數量	**2014 年有關程式數量**	**2014 年程式分類**	*2013 年讀取同等數量資料的程式數目*
8	1	遊戲	*1*
7	0	-	*3*
6	10	通訊，財經，飲食，遊戲及旅遊	*2*
5	10	娛樂，遊戲，新聞與雜誌，及旅遊及本地	*0*
4	14	娛樂，財經，飲食，遊戲，生活品味，新聞與雜誌，及旅遊及本地	*10*
3	10	書籍及參考，娛樂，遊戲，及天氣	*6*
2	11	娛樂，遊戲，新聞與雜誌，體育，工	*18*

[17]在 2014 年抽查行動後推出的 iOS8，其私隱提示已擴展至包含相機、健康、HomeKit 及運動紀錄。

讀取的私人資料類別的數量	**2014 年有關程式數量**	**2014 年程式分類**	*2013 年讀取同等數量資料的程式數目*
		具， 旅遊及本地，交通，及天氣	
1	4	書籍及參考，遊戲，生活品味， 及旅遊	*20*

42. 60 個程式可讀取的私人資料類別細分如下：

2014 年抽查結果—讀取的私人資料類別：

讀取的私人資料類別	**2014 年有關程式數量**	**2014 年程式分類**	*2013 年讀取該資料類別的程式數目*
手機獨特識別碼	50	所有類別	*44*
定位位置	39	所有類別	*36*
「發現不明的帳戶」—即手機內儲存的其他帳戶	31	書籍及參考，通訊， 娛樂，財經，飲食， 遊戲，生活品味， 新聞與雜誌，社交，旅遊及本地，及天氣	*21*
存於手機的 SMS/MMS 訊息	7	通訊，遊戲，及旅遊 及本地	*8*
使用鏡頭或錄音功能	24	娛樂，財經，飲食，遊戲，生活品味，旅遊， 新聞與雜誌，購物，社交，及工具	*10*
聯絡及／或通話紀錄	5	通訊，財經，遊戲，及旅遊	*12*
日誌內容	0	-	*1*

43. **與去年結果相比得出下述觀察：**

43.1. 依然有部分程式讀取可以用作行為及位置追蹤的私人資料—讀取手機獨特識別碼今年的數字為 83%（去年為 73%）及讀取定位位置今年的數字為 65%（去年為 60%）。雖然這些程式有否真正進行追蹤

活動不得而知，但程式開發商可以更清楚向用家解釋為何程式需要讀取這些資料，以釋除用家的疑慮；

43.2. 大部分程式仍然可透過「發現不明的帳戶」的權限來匯集、配對及串連手機用家的所有儲存於手機的帳戶—今年的數字為 52%（去年為 35%）。如程式開發商能夠匯集手機內的用家帳戶，便可以把用家的一個網上身份與其網上的其他身份結合（例如就圖一斷定 itainnoteii@gmail.com 與 Facebook 中的 Magchu May 是同一人，使用電話號碼為 5333 6069 等）。基於用家在不知情下被結合其多個網上身份有可能對其個人資料私隱有影響，程式開發商應清楚解釋為何需要如此讀取資料，並告知用家他們會否使用有關資料；及

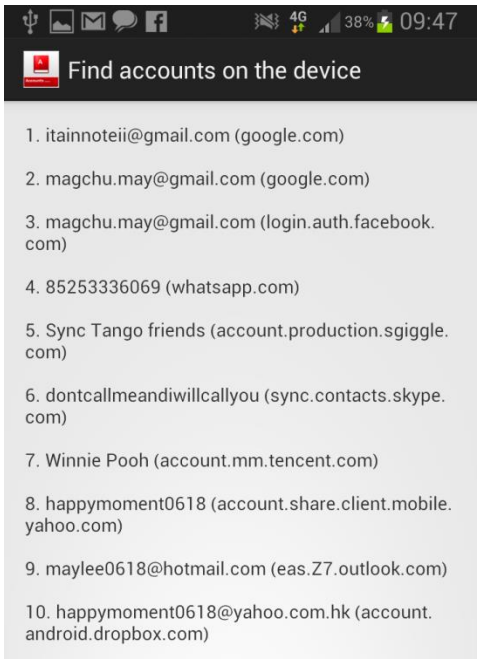


圖 1：具有「發現不明的帳戶」權限的程式可讀取儲存手機內的其他帳戶資料

43.3. 此外，今年有相當部分的程式能夠使用手機的鏡頭及錄音功能—共 40% （相比去年 16%）。雖然使用 iOS7 的手機限制在程式使用麥克風[18]前必須獲用家明確准許，但 iOS7 裝置卻沒有限制程式使用鏡頭。同樣地，Android 裝置亦沒有限制程式使用鏡頭／麥克風。基於程式開發商有可能透過鏡頭／麥克風收集敏感資料，程式開發商應清楚解釋程式何時會讀取及使用這些功能，並向用家作出保證。

[18] 在 iOS7，Apple 將私隱控制擴闊到對麥克風的使用（即在程式使用麥克風「聽取」或錄音前，會顯示訊息徵求用家准許），但 iOS7 對使用鏡頭拍照則仍然沒有作出控制。

結果一讀取記憶體

44. 在進行 2014 年抽查行動的過程中，公署發現如果 Android 程式需要讀取 Android 手機中的分享記憶體（內裏通常包含所有相片、下載檔案及其他程式在該處儲存的任何資料），該程式無需在安裝時在「權限」頁呈示任何讀取權限。這意味著很多程式在無需通知用家的情況下，便可以無限制地在 Android 手機讀取分享記憶體。

45. 這項結果令人憂慮，因為 Android 的權限模式給與的印象是在安裝程式前會在「權限」頁會呈示程式要求讀取的所有資料[19]。然而，我們的測試顯示程式可以讀取 Android 手機內記憶體的所有檔案而無須在「權限」頁中通知程式用家。

46. 為測試此權限問題，公署利用 Google 提供的基本開發裝備，在沒有使用第三者工具下編寫了一個程式並將其上載於 Google Play Store 中。該程式容許用家檢查其 Android 裝置上儲存的文件夾及檔案，以及會顯示最早 20 張儲存的相片。此程式雖然可以讀取 Android 4.3（或更早版本）裝置上的儲存相片，下載檔案，或其他程式儲存的程式或用家資料的記憶體，但在安裝過程中卻完全沒有顯示任何權限需要。下表就我們的 *File Explore* 測試程式（由 PCPD Developer 所開發）總結此漏洞:

Android 版本	「權限」頁上有否顯示任何權限需要？	可否閱讀公共記憶體內容？	可否閱讀部份內部記憶體[20]內容？
Android 4.3（或更早版本）	沒有	可以	可以
Android 4.4	沒有	不可以	可以

47. 測試程式除可閱讀公共記憶體內容外，亦可讀取任何 Android 版本上某些內部記憶體的內容。由於 Android 內部運作的複雜性，可以讀取該些內部記憶體的內容的危機暫時不詳。附錄 C 就程式 File Explore 在不同 Android 版本中可以列出甚麼資料有更詳盡的描述。

[19] http://developer.android.com/guide/topics/security/permissions.html（參考於 2014 年 12 月 10 日）

[20] 測試程式可以閱讀某部份內部記憶體，例如/system/app/ 及 /system/bin 等可能儲存有與裝置有關的敏感資料的內容。

48. 就此權限上的漏洞公署已於 2014 年 11 月 27 日正式去信 Google 敦促儘快解決。Google 回應表示 Android 4.4 或以上的作業系統已經修補了此漏洞，鼓勵用家更新。

49. 就如公署出版的《**開發流動應用程式最佳行事方式指引**》[21]所建議，程式開發商應該留意這問題，並把儲存於 Android 手機的分享記憶體中的敏感資料加密，以防止資料被讀取及外洩。

結果—發現良好的行事方式

50. 在進行 2014 年抽查行動的過程中，公署發現由香港天文台開發的「我的天文台」程式的私隱透明度及保障私隱的設計，令我們印象深刻：

50.1. 易於使用的《私隱政策聲明》—「我的天文台」在安裝程式之前、之時及之後皆有提供以短句及淺白文字撰寫，並因應細小螢幕而編寫的《私隱政策聲明》；

50.2. 相關的《私隱政策聲明》一度身訂造的《私隱政策聲明》就讀取、收集及使用甚麼資料提供精確資訊。更重要的是，該程式亦向用家保證不會讀取、收集及使用哪些可能會引起顧慮的資料。《私隱政策聲明》是以淺白文字從用家的角度撰寫，顧及他們可能關注的事宜；及

50.3. 用家逐項控制—正如第 36 及 37 段所述，Android 程式一經安裝，便可無限制地讀取已申報名單上的資料，而 iOS 程式則須至少在首次讀取某類別資料時尋求用家的權限。不過，我們發現「我的天文台」的 Android 版本（通常可無限制地讀取定位位置資料，因為已在「權限」頁的申報名單上）同時容許用家決定是否讓該程式讀取定位位置資料。在該程式的「我的位置設定」頁中，用家可以選擇是否讓該程式自動讀取手機的定位位置資料。

[21] 請參閱 http://www.pcpd.org.hk/tc_chi/resources_centre/publications/guidance/files/Mobileapp_guide_c.pdf

結論及建議

透明度不足

51. 沒有提供《私隱政策聲明》的程式數目（60 個中的 27 個）仍然高企（由去年 40%升至今年 45%）。雖然今年所有程式載有聯絡資料，但並不是全部可以藉此真正識別到程式開發商的身份。

52. 餘下 33 款有提供《私隱政策聲明》的程式則被發現有下述不足之處（詳見第 34 段）：

10 個程式 (30%)	該程式沒有提供資訊解釋會如何使用資料
11 個程式(33%)	私隱資訊不足以讓抽查者了解程式會如何使用資料
10 個程式(30%)	只有部分權限付有提供私隱資訊。抽查者因此不能完全明白程式需要某些權限的原因。

53. 60 個程式中有 34 個（57%）會顯示刊登廣告及有 30 個（50%）接受／容許／要求用家以第三者（例如社交網站）帳戶或向程式開發商開設的帳戶登入。程式開發商有可能在用家不知情或未給予同意的情況下，利用這些資料追蹤用家對廣告的行為及喜好、或建立其個人檔案及／或身份，以作日後促銷之用。這些綜合資料對促銷商而言有巨大的潛在價值，但對用家而言可以是個人資料私隱的隱憂。程式開發商應具透明度地告知用家他們會否把資料結合，並進一步使用該綜合資料。

54. 由於欠缺解釋及透明度，大部分程式（85%）在使用某些功能或讀取手機內某些資料（例如使用鏡頭及麥克風、或讀取手機獨特識別碼、定位位置、手機內其他帳戶及通訊錄）方面被視為超乎適度或超乎其表面功能。這數字大大高於環球數字的 31%。

55. 事實上，大部分程式都沒有提供足夠資訊來說服用家為何這些程式需要讀取他們表示要讀取的私人資料。

56. **建議：**公署建議程式開發商充分利用具透明度的《私隱政策聲明》，清楚地向用家說明他們會讀取、使用、傳輸及分享甚麼資料，以建立用家的信任。公署建議程式開發商參閱公署出版的《**開發流動應用程式最佳行事方式指引**》及《**保障個人資料私隱：流動應用程式開發商及其委託人須知**》[22]資料單張，以了解如何開發保障私隱的程式。

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

讀取記憶體

57. 公署發現讀取 Android 分享記憶體的程式在安裝時無需在「權限」頁告知用家。雖然此漏洞在 Android 4.4（或更新版本）已被更正，但由於市面上三分二[23]仍然使用早期版本的 Android 裝置有部份並不能更新至 Android 4.4，此漏洞仍然會為用家帶來嚴重憂慮。

58. **建議：**公署建議 Google 更正其權限模式，使用家無論在任何 Android 版本上都會被清楚提示程式會否讀取其記憶體內容。此外公署亦建議程式開發商把儲存於 Android 手機分享記憶體的敏感資料加密。

最佳行事方式例子

59. 公署發現由香港天文台研發的「我的天文台」程式提供清晰、易讀、易明及易用的《私隱政策聲明》。該程式亦讓用家另行容許該程式是否可以自動讀取儲存於 Android 手機內的定位位置資料。

60. **建議：**公署建議程式開發商參考「我的天文台」程式的功能及特點，了解開發商如何以保障私隱的態度制訂其《私隱政策聲明》。該程式亦展示讓 Android 用家容許程式讀取手機內個別資料種類是可行的（儘管 Android 手機的設計是容許程式無限制地讀取申報名單上的資料）。公署建議及鼓勵程式開發商依從同一設計理念，以提高對用家的個人資料私隱保障。

[23] 就 2014 年 12 月 1 日在 Android 儀表板 (https://developer.android.com/about/dashboards/index.html) 上得知的數據。

附錄 A – 被甄選的程式

被甄選的 **Android** 程式（以下為 **2014** 年 **5** 月 **12** 日當日的排名及下載量）

排行榜	排名	類別	程式名稱	版本	下載數量
熱門免費	6	娛樂	myTV	3.0.6	1,000,000-5,000,000
	16	通訊	StudioKUMA Call Filter 小熊來電通知	4.22	1,000,000-5,000,000
	29	旅遊及本地	KMB & LW	2.2.1	1,000,000-5,000,000
	35	工具	Octopus 八達通	3.0.1	1,000,000-5,000,000
	39	旅遊及本地	MTR Mobile	6.2.1	1,000,000-5,000,000
	60	新聞與雜誌	東網港澳	2.22	500,000-1,000,000
	62	娛樂	HK Radio 香港收音機	1.3.8.1	100,000-500,000
	72	天氣	HK District Weather 香港地區天氣	1.96	500,000-1,000,000
	74	旅遊及本地	CitybusNWFB 新巴城巴	1.5.1	500,000-1,000,000
	75	遊戲	Hong Kong Mahjong Club 雀王會正宗香港麻雀(麻將)	2.79	1,000,000-5,000,000
	77	工具	OFCA Broadband Performance Test 通訊事務管理局辦公室寬頻測試	2.0.1	500,000-1,000,000
	100	生活品味	Hong Kong Movie 香港電影	1.29.1	500,000-1,000,000
	108	新聞與雜誌	無綫新聞	1.2.1	500,000-1,000,000
	110	娛樂	Hong Kong Toolbar	2.5.5	500,000-1,000,000
	113	購物	香港格價網 Price.com.hk (手機版)	1.31	100,000-500,000
	114	生活品味	香港六合彩 (Mark Six)	4.1	1,000,000-5,000,000
	116	新聞與雜誌	RTHK On The Go	1.3	500,000-1,000,000
	131	財經	HSBC Mobile Banking	1.5.5.0	1,000,000-5,000,000
	137	財經	Money18 Real-time Stock Quote	1.7.1	500,000-

排行榜	排名	類別	程式名稱	版本	下載數量
					1,000,000
	141	財經	BOCHK 中銀香港	4.4.3	100,000-500,000
	159	交通	香港小巴	2.1.3	500,000-1,000,000
	165	社交	香討	2.91	100,000-500,000
	167	娛樂	UA Cinemas – Mobile ticketing UA Cinemas - UA 戲院手機購票服務！	2.9	500,000-1,000,000
	180	娛樂	now player now 隨身睇	3.8.20136	500,000-1,000,000
熱門收費	39	書籍及參考	Moon+ Reader Pro 靜讀天下專業版	2.5.1	100,000-500,000
最賣座	13	遊戲	火鳳燎原大戰（港澳版）	1.13	10,000-50,000
	23	遊戲	逆轉三國	5.1.4	500,000-1,000,000
	28	遊戲	嚕啊嚕	3.0.2	100,000-500,000
	55	遊戲	來自三國的你	1.8.8	100,000-500,000
	58	遊戲	萌將無雙-萱兵奪主	2.9	100,000-500,000

被甄選的 iPhone 程式（以下為 2014 年 5 月 12 日當日的排名）

排行榜	排名	類別	程式名稱	版本
熱門免費	8	天氣	MyObservatory 我的天文台	4.2.1
	9	體育	myWorldCup	1.0.1
	15	生活品味	PARKnSHOP	1.4
	33	遊戲	戲谷《三國合伙人》繁體中文版	3.0.1
	41	旅遊	85 飛的-乘客 Call 的士 App	1.2
	42	旅遊	HKTaxi 香港的士	2.0.2
	68	娛樂	熱門電視劇(港劇、美劇、台劇、韓劇、日劇、陸劇)	2.0.1
	69	飲食	元気寿司 Genki Sushi	2.4
	71	娛樂	WhatsCap - 常用對白，搞笑 CAP 圖，人氣截圖	1.1
	72	飲食	板長板前寿司 Itacho Itamae Sushi	1.2
	76	飲食	OpenRice Hong Kong 開飯喇	4.0.11
	79	飲食	OpenSnap:Food Photo Album+Nearby Search 開飯相簿: 美食相簿+附近餐廳搜尋	1.1.4
	81	新聞	蘋果動新聞	3.1.4
	82	娛樂	隨便 up	1.0
熱門收費	31	參考	牛津高階英漢雙解詞典	1.3.1
	33	旅遊	Hong Kong Taxi Translator	3.0
最賣座	3	遊戲	神魔之塔	5.03
	7	遊戲	Efun-神鵰俠侶金庸武俠正版	1.8.0
	20	遊戲	NBA 夢之隊-T-Mac 傳奇	3.0
	24	遊戲	魅子 Online	1.3.7

排行榜	排名	類別	程式名稱	版本
	30	遊戲	上古戰魂-重裝武士	2.02.04
	34	遊戲	大鬧西遊-3D 神魔．大鬧天宮	1.09.01
	35	遊戲	Efun-傾城計	2.7.0
	40	遊戲	魔物帝國	1.0.5
	41	遊戲	Efun-巨砲連隊	1.4
	43	遊戲	魔卡幻想	1.4.1
	47	新聞	SCMP Mobile Edition 南華早報手機版	2.0.2
	77	遊戲	巴哈姆特之怒-霸絶蒼穹	1.14
	84	遊戲	火鳳燎原手機版（三國卡牌）	4.2.01
	91	遊戲	我叫 MT 繁體版	3.5.4

GPEN Privacy Sweep 2014 –Sweep Form

BASIC INFORMATION				
App name	App seller / data controller	Platform	Tablet/phone	Free/Paid (if paid, how much?)

PRE-INSTALLATION METRICS		
Age / content rating	Category	Country of Data Controller

PRE-INSTALLATION COMMUNICATIONS – Please answer all applicable questions with Y/N		
Is there a privacy policy available on the app's marketplace listing? (Y/N)	If no policy in the app marketplace listing: Is there a privacy policy available on the data controller's website (Y/N)?	Does the privacy policy speak specifically to the app's collection, use or disclosure of personal information (as opposed to the data controller's practices, more generally)?[1]

PERMISSIONS – Please answer all applicable questions with Y/N	If the app does not ask for any permissions, please write 'None' here:									
	Location	Contacts	Calendar	Microphone	Camera	Device identifier (IMEI, etc.)	Access to other accounts	SMS	Call Log	Other (specify)
Does the app ask for the permission? (If N, do not answer the below)[2]										
Does the app explain how it collects, uses and discloses personal data associated with the permission?[5]										
After completing your sweep, does the permission exceed that which you would expect based on the app's functionality?[3]										

POST-INSTALLATION COMMUNICATIONS – Please answer all applicable questions with Y/N		
Is there a link to the privacy policy within the app (Y/N)?	If Y, is the privacy practice information therein consistent with the policy you saw before installing the app (Y/N)?	Do the in-app communications appear to be tailored for the 'small screen' (pop-ups, etc.) (Y/N)?[4]

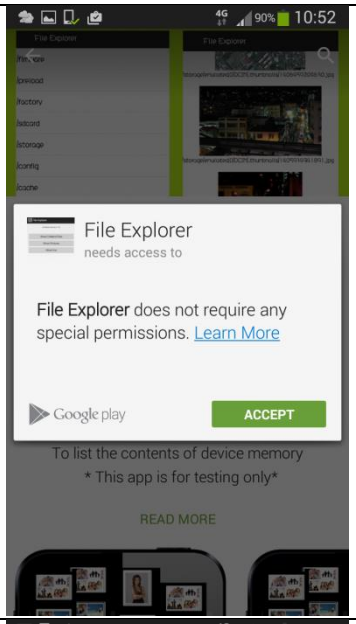
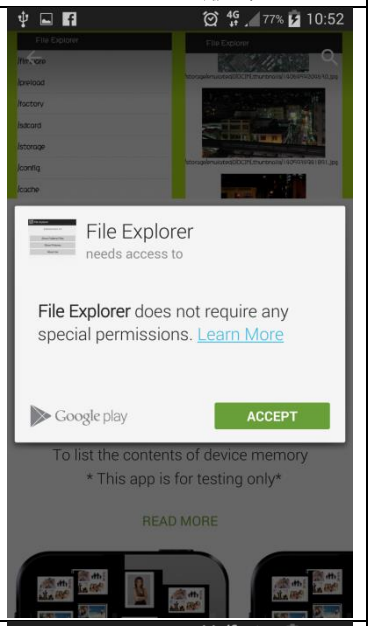
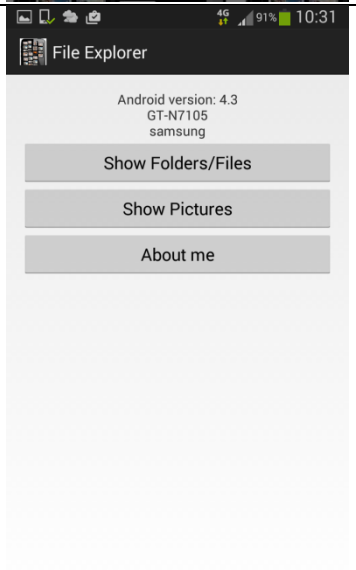
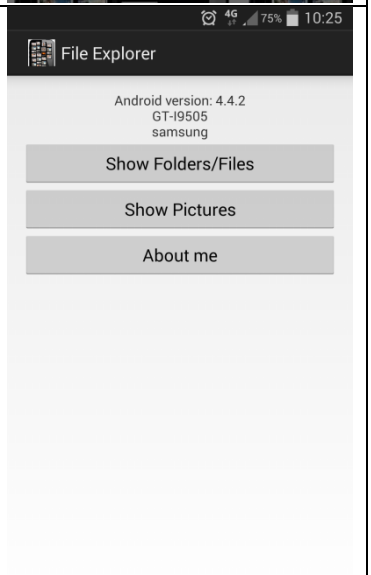
OTHER POST-INSTALLATION METRICS			
In-app ads seen (Y/N)?	Log-in requested (Y/N)?	Log-in required (Y/N)?	If log-in requested: Are you asked to create a new account, login to an existing account (Google, Facebook, etc.), or given both options?

CONCERNS (Based on sweeper's assessment)					
INDICATOR	1. The app fails, prior to installation, to explain how it will collect, use or disclose personal data? Answer: Y or N	2. Which permissions does the app request? List (or refer to above)	3. After completing your sweep, do permissions exceed that which you would expect based on the app's functionality? Answer: Y or N (and list permissions of concern)	4. Does the app fail to tailor its privacy communications for a 'small screen'? Answer: Y or N	5. Overall, the app fails to explain the permissions and how it collects, uses or discloses the associated personal data? (Answer to the below is 0, 1, 2 or 3) **N/A** = App does not collect personal information. **0** = No privacy information, other than permissions. **1** = Privacy information not adequate; sweeper does not know how information will be collected/used/disclosed. **2** = Privacy information somewhat explains the app's collection, use and disclosure of personal information, however, sweeper felt that questions remain with respect to certain permissions. **3** = Privacy information clearly explains how app collects/uses/discloses personal information; sweeper is confident in his/her knowledge about app's practices.
Response **Note: Answers based on questions noted on Sweep Form.**			Answer: List:		

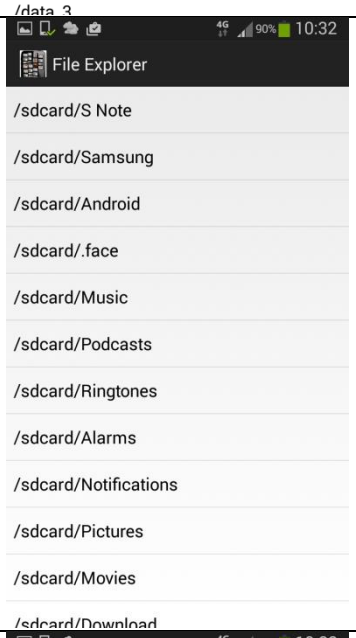
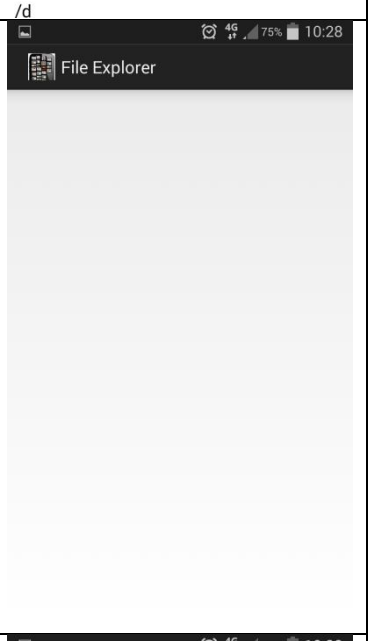
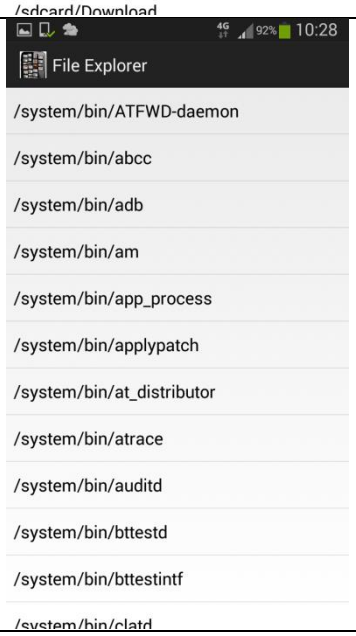
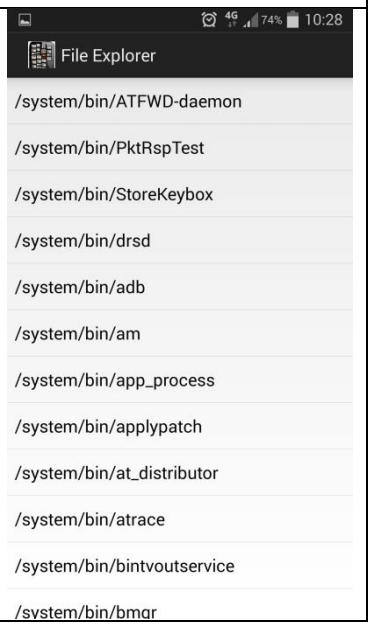
Comments - Any positive observations identified during the Sweep – whether related to the questions or not	Any concerns identified during the Sweep – whether related to the questions or not

附錄 C – 程式 File Explore 在不同 Android 版本中可以列出的資料

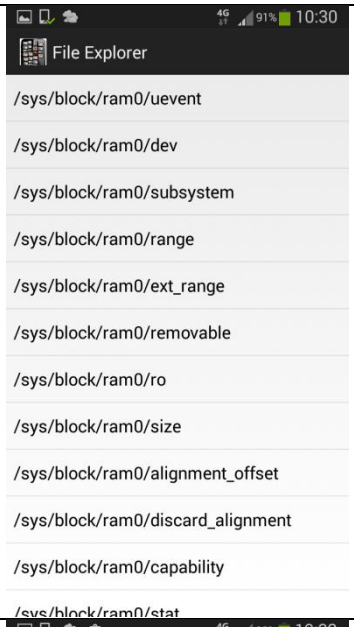
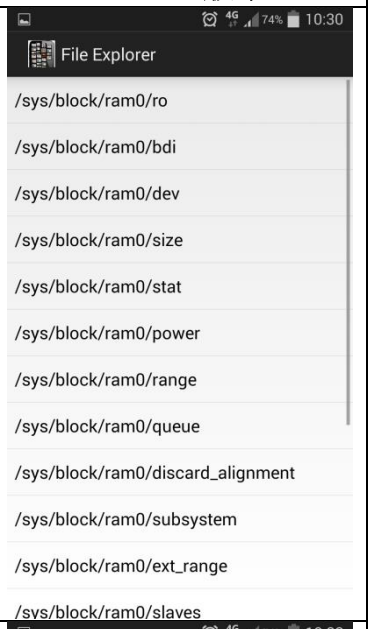
以下附表題示程式 **File Explore** 在 Android4.3 及 4.4.2 版本中可以讀取的不同資料

	Android 4.3 版本	**Android 4.4.2 版本**
安裝頁面並無顯示程式需要任何權限		
程式的首頁		

25

	Android 4.3 版本	Android 4.4.2 版本
第一層文件夾可以顯示的資料		
/sdcard 文件夾可以顯示的資料		
/system/bin 文件夾可以顯示的資料		

26

	Android 4.3 版本	Android 4.4.2 版本
/sys/block/ram0 文件夾可以顯示的資料		
程式可以顯示的相片