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

2014 Study Report on the Privacy Policy Transparency (“2014 Sweep Initiative”) of Smartphone Applications

December 2014

Table of Contents

Introduction

In May 2013 and as part of the 2013 GPEN Internet Sweep initiative[1], the Office of the Privacy Commissioner for Personal Data ("PCPD") conducted a study into the privacy policy transparency of mobile applications ("apps").

2. PCPD conducted the study on 60 most popular apps developed by Hong Kong entities and found that transparency in terms of their privacy policy was generally inadequate. Only 60% of the apps provided Privacy Policy Statements ("PPS") but even then most of them did not explain what smartphone data they would access and the purposes for the access. The PCPD subsequently published a report on the study[2] on 14 August 2013.

3. In the 2013 Sweep initiative, the PCPD was one of only two privacy enforcement authorities who chose to conduct the study in apps while the other 17 authorities looked at the privacy policy transparency of websites instead.

4. Given the proliferation and popularity of apps in recent years, all 26 privacy enforcement authorities which participated in the 2014 Sweep initiative[3] looked exclusively at the privacy policy transparency of apps.

[1] The 2013 Internet Privacy Sweep initiative ("the 2013 Sweep initiative") of the Global Privacy Enforcement Network ("GPEN") assessed the openness and transparency of corporate data users in their collection and use of personal information online (See PCPD Media Statement released on 7 May 2013: www.pcpd.org.hk/english/infocentre/press_20130507.htm). In brief, 19 privacy enforcement authorities, including PCPD, participated in the 2013 Sweep initiative with a view to increasing public and business awareness of privacy rights and responsibilities; identifying privacy concerns which need to be addressed; and encouraging compliance with privacy legislation. Each privacy enforcement authority was free to choose their scope and emphasis in the Sweep. PCPD chose to study the privacy transparency (or the lack thereof) of smartphone apps.

[2] Study Report on the Privacy Policy Transparency ("Internet Privacy Sweep") of Smartphone Applications (www.pcpd.org.hk/english/publications/files/mobile_app_sweep_e.pdf)

[3] The 2014 Privacy Sweep initiative ("the 2014 Sweep initiative") of the GPEN aims to assess corporate data users in their collection and use of personal data on mobile applications. 26 privacy enforcement authorities, including PCPD, participated in the 2014 Sweep initiative to help increase public and business awareness of privacy rights and responsibilities, identify privacy concerns which need to be addressed, and encourage compliance with privacy legislation.

Objectives

5. The 2014 GPEN Sweep initiative aims to help increase public and business awareness of privacy rights and responsibilities, identify privacy concerns which need to be addressed, and encourage compliance with privacy legislation. Specifically in terms of apps:

5.1. The study investigates how apps (or app developers) explain to consumers why they want the data they access/collect and what they will do with it; and

5.2. It examines the types of permissions apps are seeking and whether those permissions exceed what would be expected based on the apps' apparent functionality.

Sampling of Applications

6. Based on various worldwide industry figures (including PCPD's own survey published in late 2012), the majority of smartphones in use were found to be running the Google Android or Apple iOS (iPhone) operating systems. All the privacy enforcement authorities engaged in the 2014 Sweep initiative therefore decided to look exclusively at the privacy policy transparency of Android and iPhone apps.

7. Each privacy enforcement authority was free to choose the number and types of apps to be studied based on its local priority. In the case of Hong Kong, for consistency with the 2013 Sweep initiative, 30 apps from the iOS platform and 30 apps from the Android platform were chosen, and the same "Top-chart" selection criteria used last year was adopted with the aim of tracking privacy transparency trends among locally developed apps. The criteria were:

7.1. The most popular apps listed under the three top charts (Top Free, Top Paid and Top Grossing[4]) of the respective official app markets (Google Play Store for Android and App Store for iPhone);

7.2. Apps developed by Hong Kong entities; and

7.3. Apps which claimed to access any of the following private data stored or accessible on the device:

7.3.1. Unique phone identifier (such as IMEI) ;
7.3.2. Location information;
7.3.3. Account information stored on the device;
7.3.4. SMS messages stored on or to be received by the phone;
7.3.5. Camera and/or microphone functions of the phone;
7.3.6. Call logs;
7.3.7. Address book/contact details;
7.3.8. Calendar details;
7.3.9. Internal memory; and
7.3.10. List of applications running on the device.

8. The selection of the apps took place on 12 May 2014, the globally agreed starting day of the 2014 Sweep initiative. The three top charts of that day in each market were examined to identify apps that met the selection criteria. Although the original plan was to select 10 apps from each of the three top charts, there were in fact far fewer paid apps than free apps that met all criteria. Even after examining all apps under the top paid charts, it was not possible to select 10 apps in either market that met the selection criteria. As a result, proportionally more top free apps and top grossing apps were selected from App Store, and more top free apps were selected from Google Play Store to make up a total of 30 representative Hong Kong apps for each operating system.

[4] Top Free, Top Paid and Top Grossing charts in app markets show, respectively, the most popular free, paid and gross proceeds apps. These lists are refreshed/updated frequently to show the trends in different countries and locations.

9. The 60 selected apps were produced by 45 developers. The distribution of free, paid and grossing charts among them is set out in the table below.

Operating system	Top Free	Top Paid	Top Grossing	Total
Android	24	1	5	30
iPhone	14	2	14	30

10. The full list of apps selected for the 2014 Sweep initiative can be found in Appendix A. These apps were installed to Android 4.3 and iOS7 smartphones respectively for the examination.

11. During the selection, an assumption was made that if an app was available in both markets, the types of data that the app would access would be the same. This assumption was necessary because it was only possible to ascertain the types of data an Android app would access (through the Permission Page displayed during installation[5]) but not an iPhone app. As iPhone apps do not offer the same level of transparency during the installation[6] as Android apps, whether an iPhone app met the criterion of accessing certain specified information therefore had to be determined by reference to an examination of its Android equivalent.

Examination

12. The purpose of the 2014 Sweep initiative was not to conduct in-depth analysis of the design and development of apps, but rather, to examine the experience of installing and using the apps against a set of indicators.

[5] During the installation of an Android app, a "Permission Page" screen will be shown to Android users listing the types of data stored on the Android device the app has the ability to access. Users have, at that moment, the option to either continue or abort the installation (but not to select which types of data to allow the app to access). Owing to the technical architecture of Android apps, an app cannot access any type of data not "declared" on this permission page.

[6] iPhone apps do not show users what types of data they would access prior to or during the installation. However, for users of iOS 7 (the version of the iPhone operating system at the time of the study), when an app is running and prior to its access to specific types of data (specific types of data include photo album, address book, calendar, reminder, location and microphone use) for the first time, the app will prompt for permission from users to access that particular type of data. Users have the option to allow or deny the access to that type of data and the app should behave accordingly.

13. For each of the apps selected, examination was conducted in the following areas:

13.1. Is there a privacy policy statement (or equivalent) available on the app's market listing?

13.2. If there is no privacy policy statement in the app market, is there a privacy policy available on the developer's website?

13.3. Does the privacy policy statement address specifically and sufficiently the app's access, collection, use and/or disclosure of private data?

13.4. Are there any in-app advertisements?

13.5. Does the app require (mandatory) or support (optional) log-in? If affirmative, does it require a new account to be created for this purpose or use existing third party accounts (Google, Facebook etc.) or both?

14. The list of items examined for each app is listed in Appendix B. As some questions required subjective judgement on the part of those who performed the assessment (the sweepers), each app was assessed by two PCPD officers who are experienced users of the respective operating systems. Results from the two sweepers for each app were then collated and large differences resolved by a third sweeper. This arrangement was aimed at obtaining results that are representative of the typical experience encountered by smartphone users.

15. Not all questions have led to significant results but where they do, they are reported in the following sections of this report.

Results and Findings

16. Before the results are discussed, it should be noted that the app development market is probably one of the most rapidly changing environment there is. As such, the results and findings in the report should only be taken as representative of the general privacy transparency of Hong Kong apps at a particular moment in time.

17. It should also be noted that this exercise is a general survey and not in the nature of a compliance action or investigation. Without first conducting formal inquiries with each developer and spending the same level of resources on each case, it would not be appropriate to disclose adverse results and findings on specific apps at this stage.

Types of Results to be Presented

18. The results of the 2014 Sweep initiative are divided into two categories: **general results** and **specific findings**.

19. **General results** relate to overall trends and observations from all the apps. Three types of general results will be presented as follows:

19.1. **Year-by-year indicators** (availability, findability, contactability, readability and relevance) that were gathered in a similar manner in 2013 and 2014. This year's indicators are presented against last year's figures for comparison;

19.2. **2014 indicators** are indicators gathered in the Hong Kong exercise with a view to further exploring the behaviour of apps, and were only collected this year; and

19.3. **2014 global indicators** are common indicators agreed to be collected by all 2014 Sweep initiative participants as the key indicators of the exercise this year. The Hong Kong results are compared with the global results. It must be stressed again, that many of these indicators are subject to the judgement of the sweepers (e.g. whether an app fails to explain its permission requests). However, alignment of assessment results has been made by providing sweepers with examples/guidelines in the assessment form (e.g. if all permissions were explained then the answer is "yes"; if only some permissions were explained then the answer is "insufficient").

20. The following **specific findings** have serious implications on personal data privacy protection:

20.1. **Permissions** – We assessed the types of data accessible by apps and found that many of them could be used for tracking the behaviour and preferences of app users. We therefore consider it very important that app developers explain clearly why their apps need access to such data, and how the data would be further used; and

20.2. **Memory Access** – We discovered that apps with the ability to read the shared memory of an Android smartphone display no permission request during installation. This was confirmed by PCPD's own experiment in developing a test Android app. The lack of a permission request could potentially be an issue as unrestricted access to shared phone memory by apps can take place without giving any indication to app users.

21. During the 2014 Sweep exercise, we have found that the app MyObservatory has a very clear PPS and uses a privacy-friendly design, and would like to commend the app developer's efforts.

General Results – Year-on-year Indicators

22. **Availability**: Whether PPS can be found before installation or on the developer's website:

	2014 Sweep (Total = 60 apps)	***2013 Sweep (Total = 60 apps)***
PPS available on pre-installation screen[7]	15 (25%)	*0 (0%)*
PPS available at developer's website[8]	18 (30%)	*36 (60%)*
No PPS is found[9]	27 (45%)	*24 (40%)*

23. **Findability**: Whether PPS is labelled clearly on the website under a "Privacy Policy" heading:

	2014 Sweep (Total = 33 apps)	***2013 Sweep (Total = 36 apps)***
PPS not available under a "Privacy Policy" heading at the website[10]	4 (12%)	*7 (19%)*[11]

24. **Contactability**: Whether any contact information (e.g. website, phone, email, fax and/or address) is given on the pre-installation screens of apps:

	2014 Sweep (Total = 60 apps)	***2013 Sweep (Total = 60 apps)***
At least one form of contact details (email, phone, address etc.) was provided	60[12] (100%)	*36 (60%)*

25. **Readability**: Whether the PPS was easily readable:

	2014 Sweep (Total = 33 apps)	***2013 Sweep (Total = 36 apps)***
PPS was hard to read	2 (6%)[13]	*4 (11%)*[14]

[7] PPS available on pre-installation screen is by way of a link (labelled 'Privacy Policy') to developer's website.

[8] PPS available on the developer's website means there is no 'Privacy Policy' link on the pre-installation screen of the app. Sweepers obtained the developer's website either from information on the pre-installation screen or by guessing the web address.

[9] For comparison, the number of apps (that should have provided PPSs) that had provided no PPS in the 2014 global figure was 300 out of 991 apps, or 30%.

[10] PPS were found buried under links such as " Corporate Info" (公司資料), "Terms of Use" (條款及細則), "Member's Corner" (客戶專區) or "Members' Corner" (會員專區).

[11] In the 2013 Sweep, PPS were found buried under links such as "Service conditions" (服務條款), "Register to be an interactive member" (登記成為互動會員), "Customer service" (客戶服務), or "Important notice" (重要告示).

[12] The identities of five app developers could not be directly ascertained from the contact information

[13] In the two cases, the PPS was a 126-line long statement displayed in a tiny 8-line window on the developer's website.

[14] In the 2013 Sweep, two cases of PPS were available in English only but the apps were exclusively in Chinese. In the other two cases, the PPS was a 292-line long statement displayed in a 8-line tiny window on the developer's website.

26. **Relevance**: Whether the PPS presented to app users are specific to the app or generic:

	2014 Sweep (Total = 33 apps)	***2013 Sweep (Total = 36 apps)***
Number of PPS available to users during pre-installation that are written specific to apps	2 (6%)	*1 (3%)*
Number of PPS available to users after installation that are written specific to apps	3 (9%)	*2 (6%)*

27. **Compared with last year, the following observations can be made:**

27.1. The number of apps that did not provide any PPS was higher at 45% this year against 40% last year;

27.2. The availability of contact (by web-links and/or email contact) information during the pre-installation stage for apps has improved from 60% last year to 100% this year; and

27.3. The identities of some app developers were unknown this year. Even when web-links and email addresses were provided during installation, the identity of the developers for at least five apps (8%) could not be ascertained[15].

General Results – 2014 Indicators

28. **Apps serving advertisement**: 35 (58%) of the 60 apps were found to display advertisements in the app, among them 23 (38%) apps were found to display advertisements provided by third parties.

29. **Apps requiring login**: 30 (50%) of the 60 apps requested (allowed) app users to use accounts to log on to the apps to use them. Among these 30 apps, 15 (25%)

[15] Among these five apps, two of them provided links to social network pages without revealing the identities of the developers. Two others provided links to their own webpages with email address provided but the identities of the developers could not be ascertained from the webpages or the email addresses. The last one provided link to its webpage without listing any contact information.

apps allowed app users to use their third party (often social network) accounts to log on to the apps.

30. **The following observations are made from these 2014 indicators:**

30.1. There is incentive for app developers or advertisement providers to track the app users' behaviours and/or their preference over displayed advertisements. App developers and advertisement providers should be transparent in whether they do so and whether app users can opt out of this tracking by so informing app users;

30.2. Some apps that require app users to log on to use the app would allow app users to log on, more conveniently, through their social network accounts instead of through new accounts they create with the app developers. However, app developers would then have the means to combine information about the app users' behaviour or identities (where available) with their social network accounts/identities; and

30.3. None of the 30 apps that allowed app users to log on using their social network accounts had indicated whether they would combine app users' social network accounts with their behavioural data in the apps. None of the 35 apps that displayed advertisements in their apps had indicated whether they would track app users' interaction with the advertisement (such as whether and which advertisement they have opened/looked at). Apps developers should realise the potential privacy concerns and make their practices clear in their PPS to assure app users that they respect their privacy.

General Results – Comparison of local and global findings by 2014 Common Indicators

31. **Pre-installation Communication:** Concerns with respect to missing or unclear pre-installation privacy notice/communications (for example, apps providing little information about their privacy practice prior to downloading, apps providing

links that were broken or to webpages/social media pages that did not reveal the identities of the app developers, or providing only generic privacy policies not tailored to the app):

	Hong Kong **(Total = 60 apps)**	***Global*** ***(Total = 1,211 apps)***
Unclear or missing information as regards whether data would be accessed, and if yes, what data and why	43 (72%)	*715 (59%)*

32. **Small screen:** Failure to tailor privacy communications to a small screen:

	Hong Kong **(Total = 31 apps)**	***Global*** ***(Total = 1,211 apps)***
Failed to tailor privacy communications to a small screen	13 (42%)	*524 (43%)*

33. **Excessive permission:** Permissions required out of keeping with the app's apparent functionality:

	Hong Kong **(Total = 60 apps)**	***Global*** ***(Total = 908 apps)***
Permission of data access being sought went beyond user expectation based on app's functionality	51 (85%)	*281 (31%)*

34. **Overall user satisfaction:** Extent of explanation on the permissions required and how the app collected, used or disclosed information:

	Hong Kong **(Total = 60 apps)**	***Global*** ***(Total = 991 apps)***
No privacy information was provided	27 (45%)	*300 (30%)*[16]
Privacy information was available but unrelated to app	10 (17%)	
Privacy information was inadequate for sweepers to understand how the app used data	11 (18%)	*242 (24%)*
Privacy information was available in some areas but not others. Sweepers understood why some but not all permissions were required	10 (17%)	*304 (31%)*
Privacy information was provided and was clear	2 (3%)	*145 (15%)*

35. **Compared with global results, the following observations can be made:**

35.1. While the proportion of apps which failed to tailor privacy information to small screens is broadly similar between Hong Kong (42%) and global (43%) (see section 32 above), the local figures on all other counts fared worse than their global counterparts:

35.1.1. There was a higher proportion of missing/unclear pre-installation communications – locally at 72% compared with the global 59% (section 31) ;

35.1.2. The proportion of apps with possible excessive permissions was higher – locally at 85% compared with the global 31% (section 33); and

35.1.3. The proportion of apps with provision of clear privacy information was lower – locally at 3% compared with the global 15% (section 34).

[16] Not all participating authorities have differentiated the figures between *No privacy information was provided* and *Privacy information was available but unrelated to apps* so only a combined figure is available here.

Findings – Permissions

36. As in the 2013 Sweep initiative, the permissions that apps require remain a major focus this year in addition to the transparency of PPS for apps. How Android and iOS apps deal with permissions have been explained under footnotes 5 and 6 respectively. In the case of Android apps, the developer must first "declare" the types of data the app wants to access, which will then be shown to the smartphone user on the Permission Page during the installation process. The developer may declare types of data it may access when in fact the app has no access need and will not access them. However, any type of data an app would eventually access must first have been declared (otherwise Android would not allow the access), and therefore displayed to app users prior to the installation of the app.

37. In the case of iOS, there is no mechanism to show to iOS users the types of data an app intends to access, prior to or during installation. However, for smartphone owners of iOS version 7 (the version in use at the time of the study), if an app wants to access location, address book, calendar, photo album, reminder and/or use the microphone, iOS users would be prompted by a dedicated screen request[17]. They can at any time decide if they would allow a particular app's access to any of these types of data.

38. The Android platform may be considered more transparent as it shows smartphone users on the Permission Page what data will be accessed by the app before its installation. However, the Permission Page only shows what types of data will be accessed but not why such data is needed by the app. Furthermore, Android users do not have any control over what data the app can access. By installing the app, the Android user implicitly allows the app to access all data sought under declaration.

39. The iPhone platform, on the other hand, offers better granular control to smartphone users over which of the six types of data an app is allowed to access. That said, far more types of private data are stored on an iPhone the access to which the

[17] For iOS8 that was released after the 2014 Sweep initiative, this privacy protection has been extended to include Camera, HomeKit, Health and Motion Activity.

iPhone user would not know because of the lack of a comprehensive reporting mechanism like the Android platform.

40. The following parts summarise the findings regarding the types of data these 60 apps would access. As explained above, because iPhone apps do not, by design, disclose the type of data they would access, the evaluation on the types of data they access is based on the assumption that the types of data accessed on the iPhone platform are similar to that on the Android platform.

41. The number of types of data these 60 apps needed to access varied enormously. The following table gives a breakdown:

2014 Sweep Findings – Number of types of private data accessed:

Number of types of private data accessed	**Number of 2014 apps that accessed the data**	**Categories of 2014 apps**	*Number of 2013 apps that accessed the same number of data types*
8	1	Games.	*1*
7	0	-	*3*
6	10	Communication, Finance, Food & Drink, Games, and Travel.	*2*
5	10	Entertainment, Games, News & Magazines, and Travel & Local.	*0*
4	14	Entertainment, Finance, Food & Drink, Games, Lifestyle, News & Magazines, and Travel & Local.	*10*
3	10	Books & Reference, Entertainment, Games, and Weather.	*6*
2	11	Entertainment, Games, News & Magazines, Sports, Tools, Travel & Local, Transportation, and Weather.	*18*
1	4	Books & Reference, Games, Lifestyle, and Travel.	*20*

42. In terms of the types of private data these 60 apps needed to access, they can be grouped as follows:

2014 Sweep Findings – Types of private data accessed:

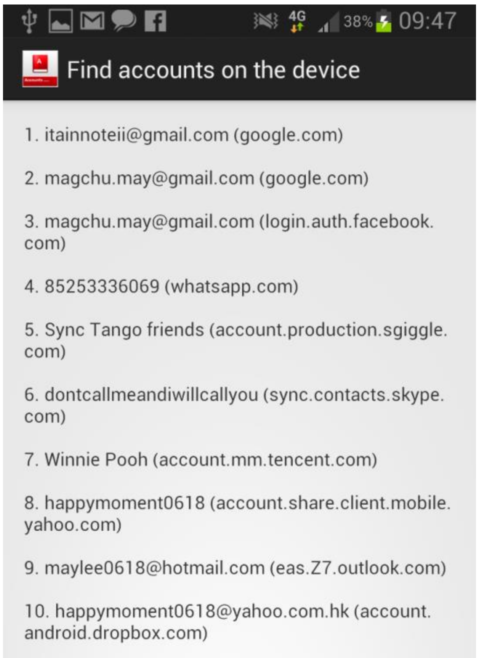
Type of private data accessed	**Number of 2014 apps that accessed the data**	**Categories of 2014 apps**	*Number of 2013 apps that accessed the data*
Unique phone identifier	50	All types.	*44*
Location information	39	All types.	*36*
Find accounts on the device	31	Books & Reference, Communication, Entertainment, Finance, Food & Drink, Games, Lifestyle, News & Magazines, Social, Travel & Local, and Weather.	*21*
SMS/MMS stored on the phone	7	Communication, Games, and Travel & Local.	*8*
Use camera and/or microphone function	24	Entertainment, Finance, Food & Drink, Games, Lifestyle, Travel, News & Magazines, Shopping, Social, and Tools.	*10*
Contacts and/or Call logs	5	Communication, Finance, Games, and Travel.	*12*
Calendar entries	0	-	*1*

43. **Compared with the findings of last year, the following observations are made:**

43.1. A large proportion of apps continues to access private data that can be used for behavioural and location tracking – 83% and 65% respectively for unique phone identifiers and locations this year against 73% and 60% last year. Whether tracking activities actually took place through these apps is unknown. App developers, however, can alleviate possible concerns by clearly explaining to app users why they need to access such data;

43.2. A large proportion of apps can potentially collate, match and correlate all the user accounts stored on smartphones (through the "Find account on device" permission) – 52% this year against 35% last year.

The ability to collate user accounts stored on a smartphone allows app developers to combine one online identity of the app user with his/her many other online identities (e.g. establishing that itainnoteii@gmail.com is the same person as Magchu May in Facebook and using the phone number 5333 6069 etc. as illustrated in Figure 1). Given the potential implication to personal data privacy for combining app users' multiple online identities without their knowledge, app developers should provide clear explanation on why their apps need such access/permission, and inform app users whether or not they would use the data; and



Find accounts on the device

1. itainnoteii@gmail.com (google.com)
2. magchu.may@gmail.com (google.com)
3. magchu.may@gmail.com (login.auth.facebook.com)
4. 85253336069 (whatsapp.com)
5. Sync Tango friends (account.production.sgiggle.com)
6. dontcallmeandiwillcallyou (sync.contacts.skype.com)
7. Winnie Pooh (account.mm.tencent.com)
8. happymoment0618 (account.share.client.mobile.yahoo.com)
9. maylee0618@hotmail.com (eas.Z7.outlook.com)
10. happymoment0618@yahoo.com.hk (account.android.dropbox.com)

Figure 1 - accounts that can be extracted by an app with the function 'Find accounts on the device'.

43.3. Furthermore, this year a good proportion of apps had the ability to use the camera and the microphone on the smartphone - 40% against 16% last year. Although in the case of smartphones running iOS7, the use of microphone[18] by an app must be explicitly allowed by the app user, this is not so in the use of camera on an iOS7 device. The use of camera/microphone in an Android device is similarly unrestricted. Given the potential to collect sensitive information through

[18] In iOS7, Apple introduced privacy control over the use of microphones (i.e. before an app can access the microphone to "listen in" or record sound, a prompt will be displayed asking for permission from users) but the use of cameras to take pictures remains uncontrolled in iOS7.

camera/microphone, app developers should provide clear explanations and assurance to app users as to when an app would access and use such functions.

Findings – Memory Access

44. In the course of the 2014 Sweep initiative, it was discovered that if an Android app needs to access the contents of the shared memory (which typically contains all the photos taken, files downloaded and any data other apps have chosen to store there) on an Android phone, the app does not need to show any access permission on the Permission Page during installation. This means many apps will have unrestricted access to the shared memory of an Android phone without notifying app users.

45. This is a cause for concern as Android had all along worked on the model that, prior to app installation, all intended access to data stored in an Android device would be fully disclosed under the Permission Page[19]. However, our tests revealed that it is possible to develop an app that can read the memory of Android devices, including photos, files, and any data other apps choose to store in the devices, without the need to inform app users through the Permission Page.

46. In our test, we developed an Android app using the standard Google-supplied development environment without any third party tools and uploaded it to Google Play Store. The app allows users to check for all the folders and files stored in an Android device, as well as displaying the first 20 photos stored. We discovered that during the installation process of our app, no permission request was shown yet the app is able to access the contents of shared memory of devices running Android 4.3 or earlier, which typically contains photos taken, files downloaded and any data other apps choose to store. The following table summarises this permission flaw discovered by using our test app *File Explorer* (developed by PCPD Developer):

[19] http://developer.android.com/guide/topics/security/permissions.html as accessed on 10 Dec 2014

Android versions on devices	**Any permission shown under Permission Page?**	**Access to shared memory?**	**Partial access to internal memory[20]?**
Android 4.3 or earlier	No	Yes	Yes
Android 4.4	No	No	Yes

47. Apart from having access to shared memory of Android devices, it was discovered that the app can also access what appears to be part of the internal memory of Android devices regardless of versions. Without knowing all the working details of Android, the impact of such access to internal memory to the security of Android devices cannot be ascertained at this stage. A more details description on what the app File Explorer can see in different versions of Android may be found in Appendix C.

48. Google was informed of this finding officially on 27 November 2014. Google responded that this vulnerability was fixed in Android version 4.4 or above, and advised users of Android devices to update to version 4.4 or above to protect themselves.

49. As stated in the PCPD published **Best Practice Guide for Mobile App Development**[21], all developers should be mindful of this issue and encrypt their sensitive data stored in the shared memory of Android phones to avoid it being accessed and risking data leakage.

Findings – Good Practice Found

50. In the course of the 2014 Sweep initiative, we were impressed by the app MyObservatory, developed by the Hong Kong Observatory, for its privacy transparency and privacy-friendly design:

[20] The app is able to read some internal memory locations showing the contents under, for example, /system/app/ and /system/bin, which may contain sensitive information about the device.

[21] See http://www.pcpd.org.hk/english/resources_centre/publications/guidance/files/Mobileapp_guide_e.pdf

50.1. User-friendly PPS – The PPS for MyObservatory uses short sentences, is written in plain language and tailored for small screens and is found to be readily available before, during and after app installation;

50.2. Relevant PPS – The tailored PPS provides precise information on what information would be accessed, collected and used. More importantly, it also assured app users what types of data with potentially concerns it would *not* access, collect and use. The PPS is written in plain language from the perspective of an app user to address their likely concerns; and

50.3. Granular user-control – As mentioned under sections 36 and 37, once installed, Android apps have unrestricted access to those data on the declared list while iOS apps must seek permission from app users at least for the first time they try to access certain types of data. We have, however, found that the Android version of MyObservatory, which would normally have unrestricted access to the location information because it is on the declared list in the Permission Page, is written in such a way that the app would allow app users to decide if the app could access location information. Under the My Location Setting page of the app, users are given the option whether to allow automatic access the app to the smartphone's location information.

Summary Conclusions and Recommendations

Inadequate Transparency

51. The number of apps (27 out of 60 apps) which did not provide PPS remained high (risen from 40% last year to 45% this year). Although contact information was published in all apps this year, not all such contact information led to identification of the app developers.

52. Among the remaining 33 apps that provided PPS, the following deficiencies were found (details may be found under paragraph 34):

10 apps (30%)	No specific information was provided on how the app would use data
11 apps (33%)	Privacy information was inadequate for sweepers to understand how the app used data
10 apps (30%)	Privacy information was available in some areas but not others. Sweepers understood why some but not all permissions were required

53. 34 (57%) of the 60 apps served advertisements and 30 (50%) of them accepted/allowed/required app users to log on using third party (such as social network) accounts or accounts they created with the app developers. App developers could use such information to track app users' behaviour and preference over advertisements and build the profile and/or the identities of app users for future marketing use without the app users' knowledge or consent. Such aggregated information has huge potential value to marketers but could be a potential personal data privacy concern to app users. App developers should be transparent in informing app users whether they carry out any combining of information and make further use of such aggregated information.

54. Owing to the lack of explanation and transparency, the majority of apps (85%) may use certain functions or access certain data stored in smartphones (such as using camera and microphone, or accessing unique phone identifier, locations, account on device and contact list) excessively or out of keeping with their apparent functions. This proportion is much higher than the global figure of 31%.

55. The fact remains that a large proportion of apps had failed to provide sufficient information to assure app users why they needed to access the private information they said they needed to access.

56. **Recommendation**: App developers are recommended to make full use of transparent PPS and explain clearly to app users what data they would access, use, transmit and share so as to build trust with app users. App developers are recommended to study the **Best Practice Guide for Mobile App Development** and

the information leaflet **Personal data privacy protection: what mobile apps developers and their clients should know**[22], published by the PCPD, for developing privacy-friendly apps.

Memory Access

57. It was discovered that apps accessing the shared memory of Android do not need to inform app users of such access on the Permission Page during app installation. Although the flaw has been corrected for Android 4.4 (and above) devices, it is still a cause for grave concern as two-third of Android users are still using devices running on earlier versions of the platform[23] and some of these devices could not be upgraded to Android 4.4.

58. **Recommendation**: Google is recommended to remedy their current arrangement so that users, irrespective which version of Android they are using, will be notified of the shared memory access permission when present in an app. In addition, app developers are recommended to encrypt sensitive data stored in the shared memory of Android smartphones.

Best Practice Example

59. The MyObservatory app, developed by the Hong Kong Observatory, was found to have a clear, easily readable and understandable, and user-friendly PPS. It was also found to have allowed app users in-app granular control over whether they would allow the app to automatically access location information stored on the Android smartphone.

60. **Recommendation**: App developers are recommended to study the MyObservatory app to see how its developer tailored, while taking into consideration the functions and features of the app, its PPS in a user-friendly manner. The app also demonstrated that it is practicable to design an app so that Android users are given

[22] See http://www.pcpd.org.hk/english/publications/files/apps_developers_e.pdf

[23] From Android Dashboard dated 1 Dec 2014: https://developer.android.com/about/dashboards/index.html

control over whether they would allow an app to access individual sets of data on an Android smartphone (despite the design of an Android smartphone allows unrestricted access to data on the declaration list). App developers are suggested and encouraged to follow the same design philosophy to enhance personal data privacy protection for app users.

Appendix A – Selected Applications

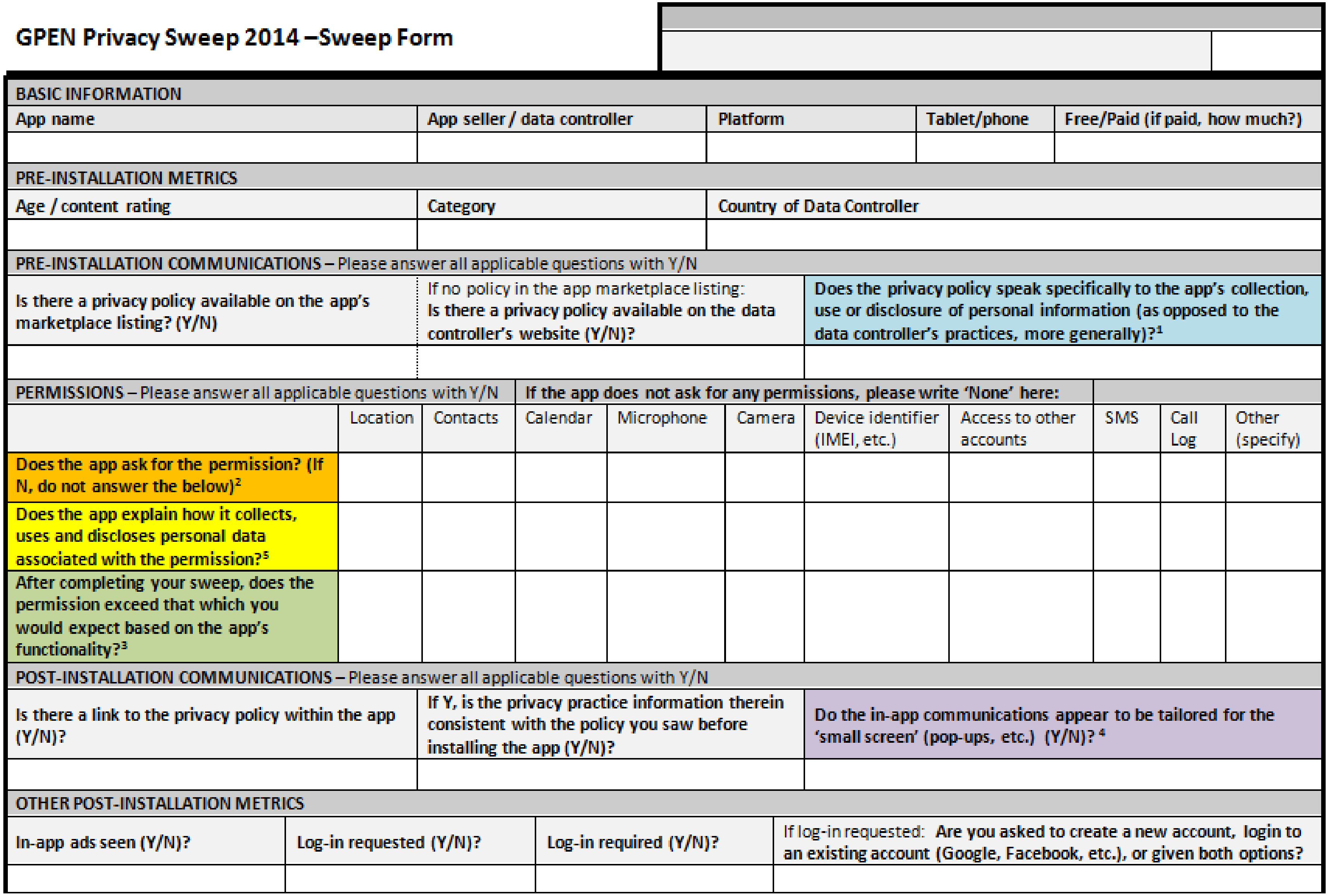
Android – Selected Mobile Apps (ranking and numbers of installation as of 12 May 2014)

Chart	Ranking	Category	Name of App	Version	No. of installs
Top Free	6	Entertainment	myTV	3.0.6	1,000,000-5,000,000
	16	Communication	StudioKUMA Call Filter 小熊來電通知	4.22	1,000,000-5,000,000
	29	Travel & Local	KMB & LW	2.2.1	1,000,000-5,000,000
	35	Tools	Octopus 八達通	3.0.1	1,000,000-5,000,000
	39	Travel & Local	MTR Mobile	6.2.1	1,000,000-5,000,000
	60	News & Magazines	東網港澳	2.22	500,000-1,000,000
	62	Entertainment	HK Radio 香港收音機	1.3.8.1	100,000-500,000
	72	Weather	HK District Weather 香港地區天氣	1.96	500,000-1,000,000
	74	Travel & Local	CitybusNWFB 新巴城巴	1.5.1	500,000-1,000,000
	75	Games	Hong Kong Mahjong Club 雀王會正宗香港麻雀(麻將)	2.79	1,000,000-5,000,000
	77	Tools	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	Lifestyle	Hong Kong Movie 香港電影	1.29.1	500,000-1,000,000
	108	News & Magazines	無綫新聞	1.2.1	500,000-1,000,000
	110	Entertainment	Hong Kong Toolbar	2.5.5	500,000-1,000,000
	113	Shopping	香港格價網 Price.com.hk (手機版)	1.31	100,000-500,000
	114	Lifestyle	香港六合彩 (Mark Six)	4.1	1,000,000-5,000,000
	116	News & Magazines	RTHK On The Go	1.3	500,000-1,000,000
	131	Finance	HSBC Mobile Banking	1.5.5.0	1,000,000-5,000,000
	137	Finance	Money18 Real-time Stock Quote	1.7.1	500,000-1,000,000
	141	Finance	BOCHK 中銀香港	4.4.3	100,000-500,000
	159	Transportation	香港小巴	2.1.3	500,000-1,000,000
	165	Social	香討	2.91	100,000-500,000

Chart	Ranking	Category	Name of App	Version	No. of installs
	167	Entertainment	UA Cinemas – Mobile ticketing UA Cinemas - UA 戲院手機購票服務！	2.9	500,000-1,000,000
	180	Entertainment	now player now 隨身睇	3.8.20136	500,000-1,000,000
Top Paid	39	Books & Reference	Moon+ Reader Pro 靜讀天下專業版	2.5.1	100,000-500,000
Top Grossing	13	Games	火鳳燎原大戰（港澳版）	1.13	10,000-50,000
	23	Games	逆轉三國	5.1.4	500,000-1,000,000
	28	Games	嚕啊嚕	3.0.2	100,000-500,000
	55	Games	來自三國的你	1.8.8	100,000-500,000
	58	Games	萌將無雙-萱兵奪主	2.9	100,000-500,000

iPhone – Selected Mobile Apps (ranking as of 12 May 2014)

Top Chart	Ranking	Category	Name of App	Version
Top Free	8	Weather	MyObservatory 我的天文台	4.2.1
	9	Sports	myWorldCup	1.0.1
	15	Lifestyle	PARKnSHOP	1.4
	33	Games	戲谷《三國合伙人》繁體中文版	3.0.1
	41	Travel	85 飛的-乘客 Call 的士 App	1.2
	42	Travel	HKTaxi 香港的士	2.0.2
	68	Entertainment	熱門電視劇(港劇、美劇、台劇、韓劇、日劇、陸劇)	2.0.1
	69	Food & Drink	元気寿司 Genki Sushi	2.4
	71	Entertainment	WhatsCap - 常用對白，搞笑 CAP 圖，人氣截圖	1.1
	72	Food & Drink	板長板前寿司 Itacho Itamae Sushi	1.2
	76	Food & Drink	OpenRice Hong Kong 開飯喇	4.0.11
	79	Food & Drink	OpenSnap:Food Photo Album+Nearby Search 開飯相簿: 美食相簿+附近餐廳搜尋	1.1.4
	81	News	蘋果動新聞	3.1.4
	82	Entertainment	隨便 up	1.0
Top Paid	31	Reference	牛津高階英漢雙解詞典	1.3.1
	33	Travel	Hong Kong Taxi Translator	3.0
Top Grossing	3	Games	神魔之塔	5.03
	7	Games	Efun-神鵰俠侶金庸武俠正版	1.8.0
	20	Games	NBA 夢之隊-T-Mac 傳奇	3.0
	24	Games	魅子 Online	1.3.7
	30	Games	上古戰魂-重裝武士	2.02.04
	34	Games	大鬧西遊-3D 神魔．大鬧天宮	1.09.01
	35	Games	Efun-傾城計	2.7.0
	40	Games	魔物帝國	1.0.5
	41	Games	Efun-巨砲連隊	1.4
	43	Games	魔卡幻想	1.4.1
	47	News	SCMP Mobile Edition 南華早報手機版	2.0.2
	77	Games	巴哈姆特之怒-霸絕蒼穹	1.14
	84	Games	火鳳燎原手機版（三國卡牌）	4.2.01
	91	Games	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?)

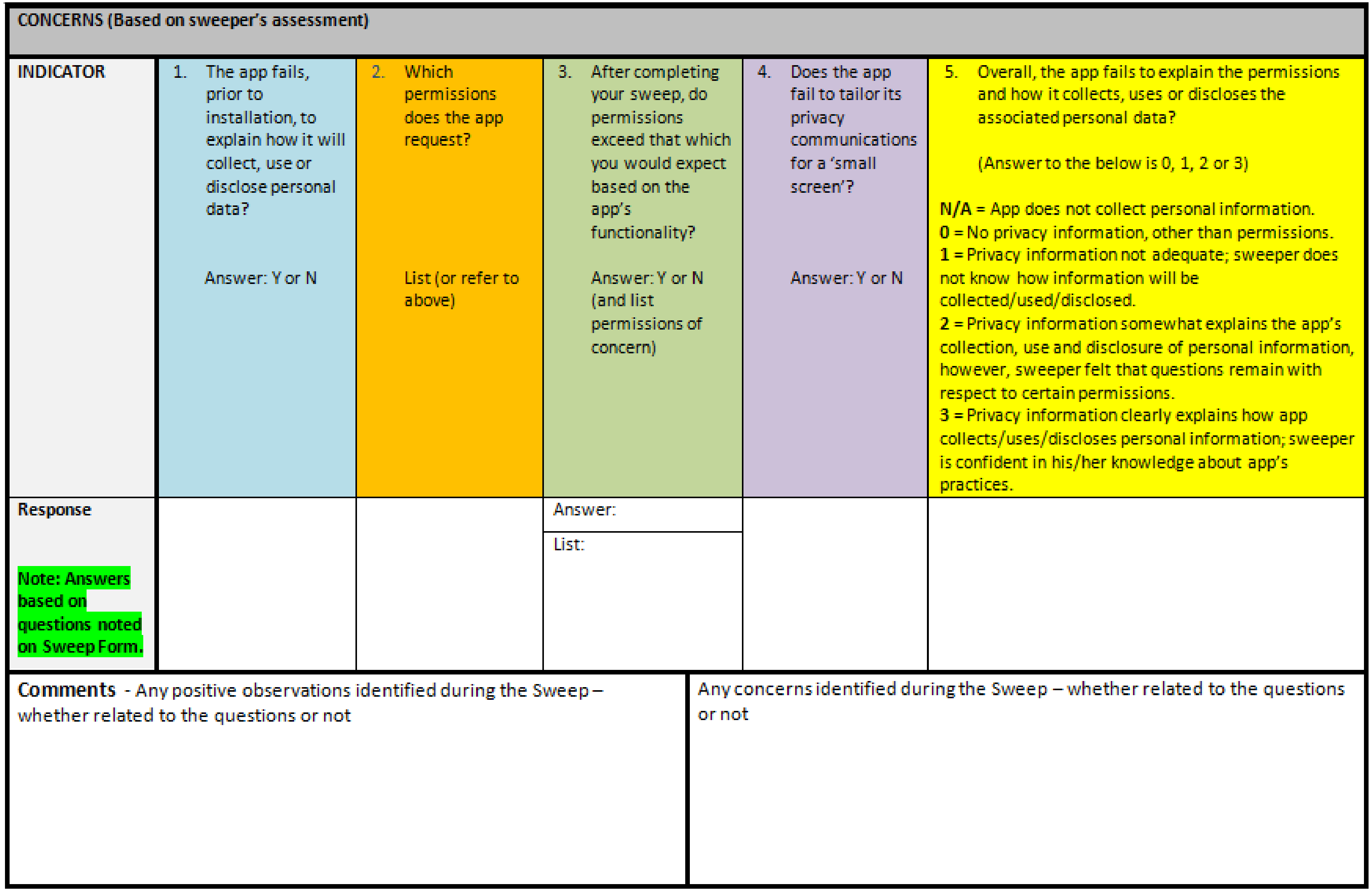
PRE-INSTALLATION METRICS		
Age / content rating	Category	Country of Data Controller

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]

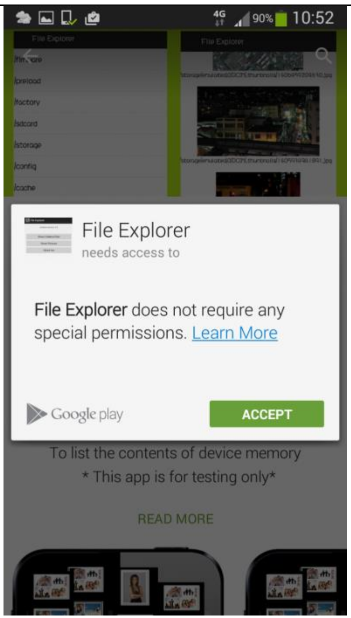
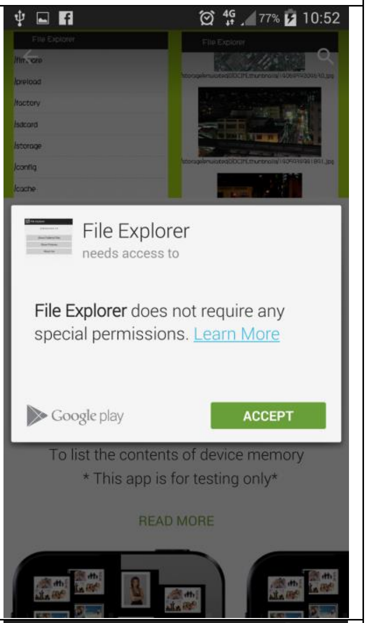
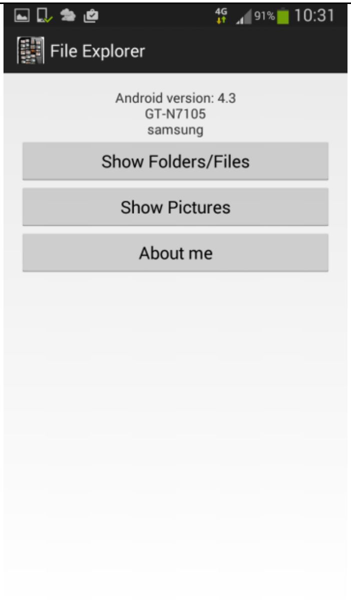
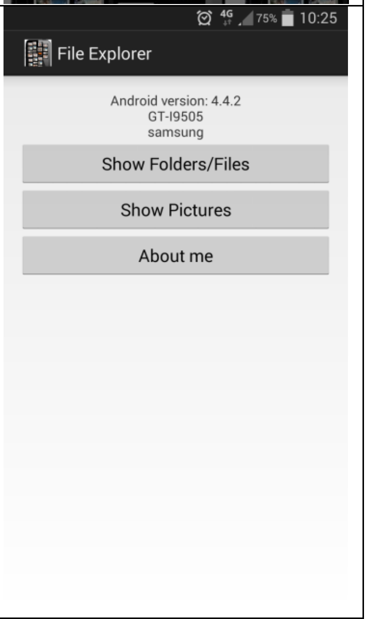
OTHER POST-INSTALLATION METRICS			
In-app ads seen (Y/N)?	Log-in requested (Y/N)?	Log-in required (Y/N)?	If log-in requested: Are you asked to create a new account, login to an existing account (Google, Facebook, etc.), or given both options?

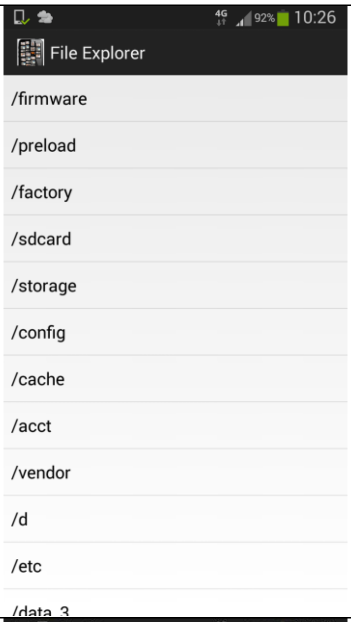
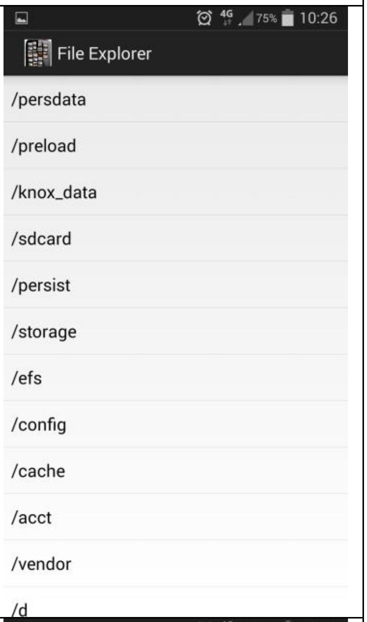
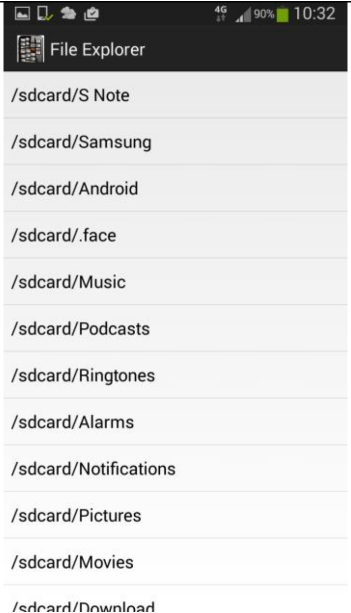
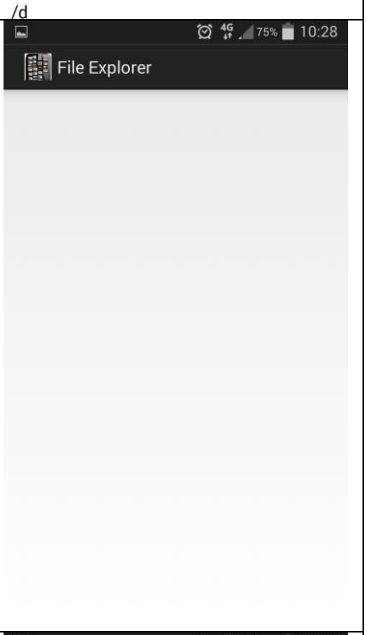
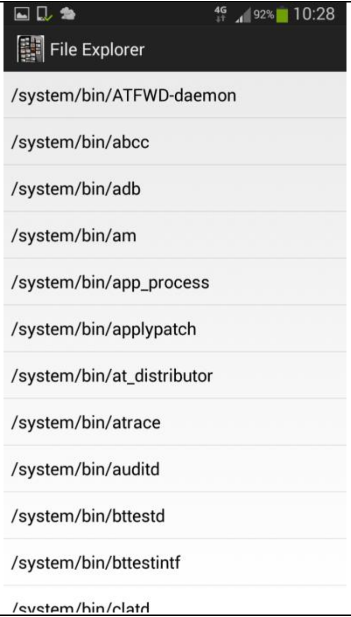
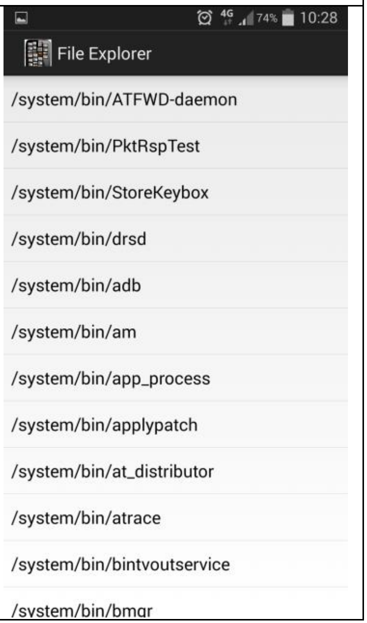


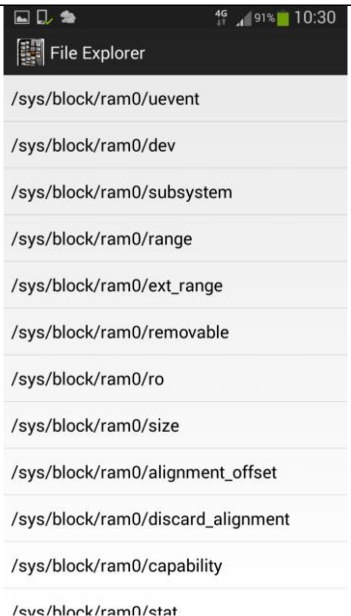
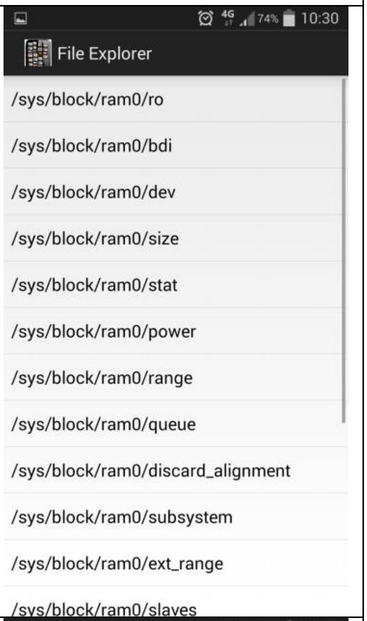
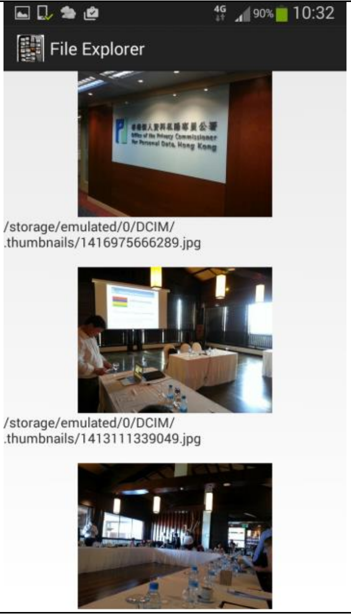
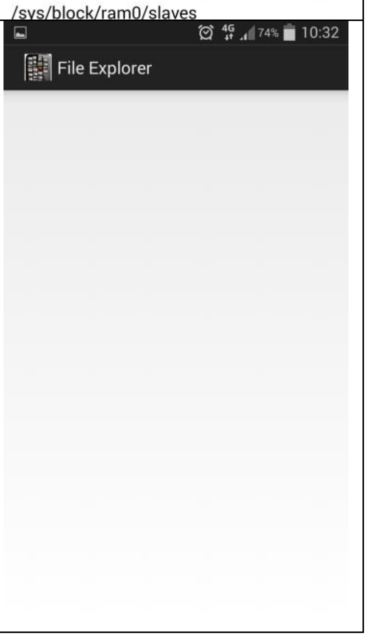
CONCERNS (Based on sweeper's assessment)					
INDICATOR	1. The app fails, prior to installation, to explain how it will collect, use or disclose personal data? Answer: Y or N	2. Which permissions does the app request? List (or refer to above)	3. After completing your sweep, do permissions exceed that 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		

Appendix C – Information shown in File Explorer under two versions of Android

The following table shows the different types of information accessible by the app **File Explorer** when running under Android versions 4.3 and 4.4.2

	Android versions 4.3	Android versions 4.4.2
Installation screen showing no permission is required by the app	 File Explorer needs access to File Explorer does not require any special permissions. Learn More Google play ACCEPT To list the contents of device memory * This app is for testing only* READ MORE	 File Explorer needs access to File Explorer does not require any special permissions. Learn More Google play ACCEPT To list the contents of device memory * This app is for testing only* READ MORE
Opening screen	 File Explorer Android version: 4.3 GT-N7105 samsung Show Folders/Files Show Pictures About me	 File Explorer Android version: 4.4.2 GT-I9505 samsung Show Folders/Files Show Pictures About me

	Android versions 4.3	Android versions 4.4.2
Displayable contents in the first-level folder	 4G 92% 10:26 File Explorer /firmware /preload /factory /sdcard /storage /config /cache /acct /vendor /d /etc /data_3	 4G 75% 10:26 File Explorer /persdata /preload /knox_data /sdcard /persist /storage /efs /config /cache /acct /vendor /d
Displayable contents in the /sdcard folder	 4G 90% 10:32 File Explorer /sdcard/S Note /sdcard/Samsung /sdcard/Android /sdcard/.face /sdcard/Music /sdcard/Podcasts /sdcard/Ringtones /sdcard/Alarms /sdcard/Notifications /sdcard/Pictures /sdcard/Movies /sdcard/Download	 4G 75% 10:28 File Explorer
Displayable contents in the /system/bin folder	 4G 92% 10:28 File Explorer /system/bin/ATFWD-daemon /system/bin/abcc /system/bin/adb /system/bin/am /system/bin/app_process /system/bin/applypatch /system/bin/at_distributor /system/bin/atrace /system/bin/auditd /system/bin/bttestd /system/bin/bttestintf /system/bin/clatd	 4G 74% 10:28 File Explorer /system/bin/ATFWD-daemon /system/bin/PktRspTest /system/bin/StoreKeybox /system/bin/drsd /system/bin/adb /system/bin/am /system/bin/app_process /system/bin/applypatch /system/bin/at_distributor /system/bin/atrace /system/bin/bintvoutservice /system/bin/bmgr

	Android versions 4.3	Android versions 4.4.2
Displayable contents in the /sys/block/ram0 folder	 File Explorer /sys/block/ram0/uevent /sys/block/ram0/dev /sys/block/ram0/subsystem /sys/block/ram0/range /sys/block/ram0/ext_range /sys/block/ram0/removable /sys/block/ram0/ro /sys/block/ram0/size /sys/block/ram0/alignment_offset /sys/block/ram0/discard_alignment /sys/block/ram0/capability /sys/block/ram0/stat	 File Explorer /sys/block/ram0/ro /sys/block/ram0/bdi /sys/block/ram0/dev /sys/block/ram0/size /sys/block/ram0/stat /sys/block/ram0/power /sys/block/ram0/range /sys/block/ram0/queue /sys/block/ram0/discard_alignment /sys/block/ram0/subsystem /sys/block/ram0/ext_range /sys/block/ram0/slaves
Displayable contents in the photo folder	 File Explorer /storage/emulated/0/DCIM/.thumbnails/1416975666289.jpg /storage/emulated/0/DCIM/.thumbnails/1413111339049.jpg	 File Explorer