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

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

August 2013

Table of Contents

Background

The Office of the Privacy Commissioner for Personal Data (PCPD) commissioned The Centre for the Advancement of Social Science Research of the Baptist University to conduct a survey on privacy awareness on smartphones and smartphone apps[1] (the privacy survey for smartphones) in 2012. The results of the survey show that 57% of the 1,013 respondents did not know or were not sure what information their apps had access to, and 51% of the respondents did not know that their address books might be uploaded to a central server when using social network apps. Furthermore, only 27% of the respondents would consider the privacy policy of an app before installing it, and 50% of the respondents were not worried about data leakage risks when using smartphones or installing apps.

2. The results of the survey suggest that smartphone users were not aware of the potential privacy intrusion to them when using smartphones or smartphone apps.

3. Smartphones store a range of data that are close and dear to the individuals who use them. For example, a smartphone may store its locations over a period of time thus exposing the trails of its owners. It may also contain very private pictures or messages of the owner. Its address book not only contains contact information of many people, but also potentially reveals the relationship between these people and the owner.

4. Importantly, when combined with other information, data stored in the smartphone could potentially reveal a great deal about the owner. For example, if an app collects the unique identifier of a smartphone, and it records whether a user clicks on the advertisement it displays, its developer would be able to build a profile of the user's interests over time unbeknown to the user. If such information is shared among many app developers, the value of the information would become even greater to them or marketers.

5. It is therefore important that apps developers are as open and transparent as possible to smartphone users as to what their apps would access, and why and when such access is necessary. Only with a good level of transparency would smartphone users be given sufficient information to make an informed decision on whether to install or use an app.

6. It is with this in mind that the PCPD conducted a study[2] in May 2013, to determine the level of privacy transparency of apps available in the market.

[1] Report on Privacy Awareness Survey on Smartphones and Smartphones Apps (www.pcpd.org.hk/english/publications/files/smartphone_survey_e.pdf)

[2] This study also formed part of the Internet Privacy Sweep initiative ("the Sweep") of the Global Privacy Enforcement Network ("GPEN") to assess 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, nineteen privacy enforcement authorities, including PCPD, are participating in the Sweep 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. Given the concerns

Objectives

7. The study aims to:

7.1. find out if apps developers provide privacy policy statements (PPS) to smartphone users prior to the installation of the apps;

7.2. find out the level of privacy transparency of apps provided to smartphone users (this may include the type of data to be accessed by an app, the reason for such access and under what circumstances the access would take place); and

7.3. find out the typical types of data to be accessed by apps, and to remind members of the public of the potential privacy risks when using apps.

Sampling of Applications

8. Given that the PCPD survey on privacy awareness on smartphones and smartphone apps revealed that the majority (over 80%) of smartphone respondents used Android or iPhone operating systems, this study of apps has concentrated on studying the privacy transparency of Android and iPhone apps.

9. The official app markets of these operating systems, Google Play Store for Android and App Store for iPhone, offer 'Top Charts' showing the more popular apps being downloaded. The top charts shown in these stores typically include Top Free, Top Paid and Top Grossing categories.

10. Each of these top charts under App Store contains up to 300 apps and those under Google Play Store, 500 apps. Only apps developed by Hong Kong data users were included in the study. This was determined by examining whether the published developers of the apps were Hong Kong entities. It was decided that 10 apps would be selected from each of these charts in each operating system to be assessed, resulting in 60 apps (i.e. 30 apps from each operating system) to be studied in total.

11. This being a study of personal data privacy, only apps that claimed to access any of the following private data were included in the study:

11.1. Phone status and unique phone identifier (IMEI number) ;
11.2. Location information of the phone;
11.3. Account information stored in the phone;
11.4. List of applications running in the phone;
11.5. SMS/MMS messages stored or to be received by the phone;
11.6. Camera and/or microphone functions of the phone;
11.7. Call logs;
11.8. Address book/contact details;
11.9. Calendar details; and
11.10. Sensitive system logs.

over smartphone apps mentioned above, PCPD chose to study the privacy transparency or the lack thereof of smartphone apps.

12. The selection of the apps took place on 6 May 2013, the globally agreed starting day of the Sweep exercise. It was then discovered that there were far fewer paid Hong Kong apps than free Hong Kong apps that met all selection criteria. Even after exhaustively examining all apps under the Top Paid and Top Grossing charts, it was not possible to select 10 apps from each of these charts that met the selection criteria. As a result, more Top Free apps were selected until 30 Hong Kong apps were selected from each operating system. The eventually selected 60 apps were developed by 40 developers.

13. The full list of apps selected on 6 May 2013 for the study can be found in Appendix A.

14. The following numbers of apps were selected from the charts of the two operating systems on 6 May 2013. These were Hong Kong apps and all accessed the types of private data listed under para 11:

Operating system	**Top Free**	**Top Paid**	**Top Grossing**	**Total**
Android	21	2	7	30
iPhone	22	4	4	30

15. During the selection, an assumption was made that when an app was available in both operating systems, the types of data that the app accessed would be the same. This assumption was made because it was only possible to ascertain the types of data an Android app accessed but not an iPhone app. This is because the types of data to be accessed by an Android app would be shown explicitly under the Permission page prior to its installation[3]. As iPhone apps do not offer the same level of transparency at the outset[4], whether an iPhone app met the criterion of accessing certain specified information was determined by examining its Android equivalent.

Examination

16. For each of the apps selected, examination was conducted on the pre-installation screens to examine the adequacy of privacy notice (if any) and level of transparency. If insufficient information was available on the pre-installation screen, attempt would be made to access the developers' website to examine the adequacy of

[3] During the installation of an Android app, a screen of "Permission" will be shown to Android user listing the types of data stored in 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). Due to the technical architecture of Android apps, an app cannot access any type of data not "declared" in this permission page.

[4] iPhone apps do not show users what types of data they would access prior to or during the installation. However, for users of iOS 6 (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 and location) 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.

privacy notice and level of transparency. Specifically any PPS relevant to the app would be identified.

17. Finally apps were loaded to the respective smartphones in order to access their functions and any further privacy-related information.

18. Appendix B shows the full list of items examined in each app.

Findings

19. Before the findings are discussed, it should be noted that the app development market is probably one of the most rapidly changing environment there is. For example, one app was upgraded just two days after it was selected, and numerous others have also been upgraded between they were selected and this report is made public. As such, the 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.

20. It bears specific emphasis that this exercise is a general survey and not in the nature of a compliance action or investigation. Without spending the same level of resources on each case and to make formal enquires with each developer, it would not be appropriate to disclose findings on specific apps at this stage. All findings in this report are therefore derived from aggregated statistics.

General Findings

21. **Availability**: No PPS was found (not in pre-installation screens, not in websites and not in the apps) in 24 (40%) out of 60 apps studied. The remaining apps (36, or 60%) made their PPS available on their websites.

22. **Findability**: Out of the 36 apps with PPS, 7 (19%) websites did not list them under the usual privacy policy/statement links on the home pages. Instead, they were found buried under links such as 服務條款 (service conditions), 登記成為互動會員 (register to be an interactive member), 客戶服務 (customer service), or 重要告示 (important notice).

23. **Contactability**: Out of the total 60 apps, 24 (40%) of them had not provided any form of contact information (e.g. website, phone, email, fax and/or address) on their pre-installation screens.

24. **Readability**: Out of the 36 apps with PPS, two (2) (6%) had PPS in English only but the apps were exclusively in Chinese, and two (2) (6%) had an astounding 292-line PPS displayed in a tiny 8-line window on the developer’s website.

25. **Relevancy**:

25.1. Two (2) apps had app-specific PPS developed in addition to the website PPS but they could only be found in the apps after they were installed.

25.2. One (1) app did not show PPS prior to installation (not on pre-installation screen, not on web site) but an app-specific PPS was available in the app after installation.

25.3. Out of the 36 apps that had PPS, 33 (92%) of them only provided generic PPS to smartphone users. Many of these PPS referred only to arrangements clearly applicable in the physical world. For those that made reference to the collection and use of personal data online, they only made reference to cookies but not data that are specific to smartphones such as locations and IMEI numbers etc.

A Matter of Permission

26. While PPS is an important means to inform smartphone users about the developer's privacy policies and practices in relation to the personal data it handles, it is equally important that smartphone users are made aware of the types of data an app would be able to access.

27. How a smartphone user is informed of what data an app will access vary across different operating systems. In the case of Android apps, the developer must first "declare" the types of data the app wants to access, which will be shown to the smartphone user on the Permission page prior to installation of the app, before such data can be accessed by the app (see footnote 3). The developer may declare more types of data it may access even if the app does not in fact and has no need to access them. However, any data an app can successfully access must first be declared and displayed to smartphone users prior to the installation of the app.

28. In the case of iPhone, there is no mechanism to show to iPhone users what an app intends to access, prior to, during or after installation. However, for smartphone owners of the iOS version 6 (the version in use at the time of the study), if an app wants to access location, address book, calendar, photo album and/or reminder, they would be prompted by a dedicated screen request. Smartphone users can at any time decide if they would allow a particular app's access to any of these types of data (see footnote 4).

29. The Android platform is more transparent as it shows smartphone users in the Permission page what data an app will access before its installation. However, the Permission page only shows what type of data is being accessed but not why such data is needed by the app. Furthermore, smartphone users do not have any control over which data the app can access. By installing the app, the smartphone user allows the app to access all declared data.

30. The iPhone platform, on the other hand, offers granular control to smartphone users to decide which of the five types of data an app is allowed to access. That said, there are far more types of private data stored on an iPhone the access to which the smartphone user would not know because of the lack of a comprehensive reporting mechanism like the Android platform.

31. The following parts summarise the findings regarding the types of data these 60 apps declared that they would access. As mentioned before, iPhone apps do not, by design, disclose what type of data they would access. All iPhone apps were assessed by examining the permissions declared by their available Android versions. The findings are, therefore, based on the assumption that the type of data accessed by the same app on the iPhone platform is the same (or similar) as that of the Android platform).

32. The types of data these 60 apps needed to access varied enormously. The following table gives a breakdown of the apps by the number of private data accessed (highest to lowest):

Number of private data accessed	Number of apps that accessed the data	Categories of apps
8	1	Games
7	3	Games
6	2	Communication and Lifestyle
4	10	Games, Entertainment, Finance, Business, Education and Utilities
3	6	Games, Entertainment, Lifestyle and News
2	18	All above types
1	20	All above types

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

Type of private data accessed	Number of apps that accessed the data	Categories of apps
IMEI number	44	All types
Location information	36	All types
Find accounts on the device	21	Games, Entertainments, Food & Drink, Lifestyle, News, Utilities, Finance, Education and Communication
SMS/MMS stored on the phone	8	Games
Use camera and/or microphone function	10	News, Entertainment, Games, Social, Utilities, Education and Business
Call logs	6	Games, Communication and Lifestyle
Address books	6	Games, Communication and Lifestyle
Calendar entries	1	Lifestyle

34. **Locations**: Thirty-six (36) (60%) of the total 60 apps were able to access the location information on the phone. While the privacy intrusiveness of obtaining location information alone may be arguable, 25 (42% of the 60 apps) of these 36 apps were also able to access the IMEI number, and 20 (33% of the 60 apps) of these 36 apps required or optionally allowed smartphone users to log on to the app. Location information would become a lot more meaningful when it is combined with IMEI number (which may be obtained or shared by other apps) or physical account (where rather detailed personal data could have been collected by the developers or their partners).

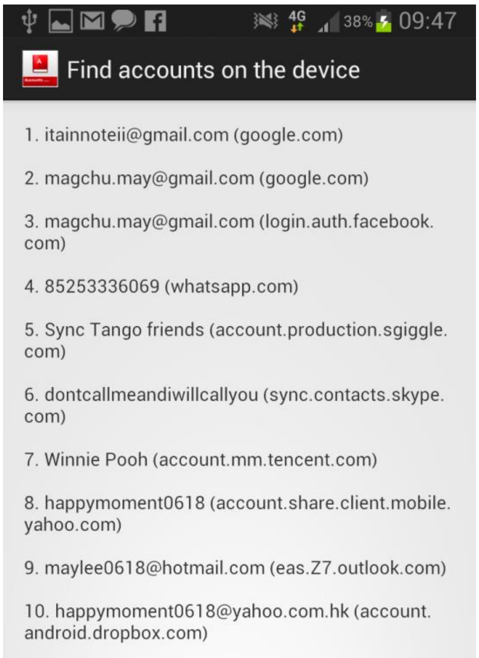
35. **Behavioural Tracking**: Forty-four (44) (73%) apps were able to access the phone's IMEI number. The potential privacy intrusiveness of this would depend on what other information the app was able to collect. Apart from the fact that 25 (42% of the 60 apps) of these 44 apps were capable of accessing the location information, 10 (17% of the 60 apps) were able to find out what other apps were running on the phone, and 19 (32% of the 60 apps) showed third-party advertisements with the app. All such combinations of access or actions could allow the developers to track the smartphone users' behavioural preferences and interests.

36. **Contacts, Call Logs and Calendar Access**: Six (6) (10%) apps were able to access the full address book stored on the phone. The same six apps were also able to read the call logs stored on the phone, and one could concurrently access the calendar. Four of these six apps were games.

37. **Account Access**:

37.1. Twenty-one (21) (35%) apps were able to access the full list of accounts stored on the phone (Find accounts on the device). This meant an app would know what other accounts were stored on the phone. 13 (22% of the 60 apps) of these 21 apps were concurrently able to access the location information of the smartphone.

37.2. To demonstrate the power of this access, a test app was developed by the PCPD to see what information could be accessed. Fig 1. shows how such access allows an app to extract all other accounts (and their respective services) from the smartphone:



38% 09:47

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'.

37.3. Whether combined with other types of access such as locations or not, this ability to see other accounts stored on the smartphone would allow the developers to collect a multitude of identities used by the same smartphone user and understand their correlation.

38. **SMS/MMS Access**: Eight (8) (13%) apps were able to access the full contents of SMS/MMS messages stored on the phone. Exclusively all these apps were games.

39. **Camera/Microphone Access**: Ten (10) (17%) apps were able to use the camera and/or the microphone function of the phone. While there were obvious reasons for some of these apps to do so, no app developer had explained under what circumstances would picture or voice be taken or recorded.

40. **Permission Declaration**: Three (3) (5%) apps had dedicated privacy policy statements for their apps but all of them were only shown after the apps were installed. One of these apps had the policy listed under FAQs (常見問題) in the app. One of these three apps explained in the description of the pre-installation screen what permissions it required and why those permissions were required. However, this was only found if the language of the smartphone was set to Chinese. When the language of the smartphone was changed to English, the pre-installation description would be switched to English but the description on permissions was missing. In any case, the description was limited to the listing of the permissions as opposed to the full privacy policy.

Conclusions and Privacy Implications

Inadequate transparency

41. This study brings to the fore the uncertainty in the personal data processing practice of these apps by their developers. This conclusion of lack of transparency is underpinned by the following observations:

> 41.1. After efforts made in searching, only 36 (60%) apps had PPS available on the developers' websites. Yet only one of these was a PPS written specifically for apps. The other 35 PPS made no mention of the collection and handling of private data on the smartphones, such as the IMEI number, locations, other accounts stored, call logs etc.

Potential risks to personal data privacy

42. While taken individually, each type of data stored on a smartphone would only reveal very little information about the user of the smartphone, a combination of such data would paint a very different picture. While a third of the 60 apps needed only to access one type of data, many of them required to access many more. A number of privacy risk implications arise:

> 42.1. Is it really necessary to record the phone's IMEI number to operate an app? The collection of IMEI number would allow developers to potentially correlate many types of data. It would be particularly valuable if physical data, such as location or accounts, could be collected and correlated at the same time. It would be even more valuable if such data is shared among developers. For example, if one app collects the IMEI number and the locations of the smartphone, and another app (whether by the same developer or another) collects the IMEI number of the phone and Facebook account name on the smartphone, and if such data is combined the locations of an individual could be revealed even when he/she had specifically switched off the location tracking mode for his Facebook account.
>
> 42.2. If an app also serves third-party advertisements, the developer may have the ability to track and profile smartphone users. For example, if an app collects the IMEI number, the app would be able to track which advertisements the user has clicked and thereby build up a perceived preference/profile of certain categories of interests of that user. Are users aware of this categorisation of themselves and do they have the ability to opt out of future tracking/profiling or categorisation? This may be of particular concern if a user disagrees with the category he/she has been assigned and finds no way of rectification.
>
> 42.3. If an app requires or supports smartphone users to log on the app, the developer could be in a position to correlate smartphone data with physical accounts (that contain personal data) and obtain a better profile of an

individual. This can be a way of knowing an individual ‘by the back door’. For example, an app may now be able to associate location data and contact details (in some cases, relationship as well if such information is recorded in the address book) with a physical account without the user realising that such information is being collected and stored. Is the individual aware of this and is he/she offered the right of self-determination in such cases?

42.4. Address books, call logs, calendar entries, and SMS/MMS messages are often very personal and private to smartphone users. Is the access to these types of data really necessary, particularly for games? It is also uncertain what the developers would do with such information accessed. For example, would they upload such information to a central server (or share the information with other users of the same app platform)? Would the user be notified of the action (and the extents of the sharing) and have the opportunity to opt-out?

42.5. The use of camera and microphone of the smartphone by many apps appeared to be necessary. However, many spyware could pose as apps that require access to these functions and so beyond the normal use to take pictures or voice recordings at any time without the user’s knowledge. Should developers be more transparent in their practice and tell users when and for what purpose will they use the smartphone’s camera and microphone?

42.6. The study reveals that the ability to access the information of other accounts stored in a smartphone is a powerful and worrying one. This was demonstrated by the test app the PCPD developed for this exercise. Once a user accepts an app with the ability to ‘find accounts on the device’, it can extract many other accounts installed/used on the smartphone. In the case demonstrated in Figure 1, information such as the phone number (usually the account name stored in Whatsapp), and multiple email accounts (for services such as Gmail, Outlook, Yahoo) can be extracted, and one’s identities across multiple services will be revealed without the individual realising. The purpose and extent of use by developers of this function should be clearly explained to users to ease concerns.

43. In summary, the level of transparency was low and unsatisfactory, and smartphone users could not make an informed decision on whether they should exchange their personal data stored on their smartphone (or entered as part of the process of using the app) for the benefits (or risks) of using the app.

Recommendations

44. App developers are recommended to improve the level of transparency by:

44.1. adopting the privacy-friendly design approach and limit the type of data to be accessed by their apps to what is necessary;

44.2. incorporating app-specific PPS at the pre-installation screen (or make them readily available prior to the user installing the app);

44.3. explaining in their PPS what type of data they would collect and handle, and under what circumstances would such collection and handling take place; and

44.4. addressing their minds to the concerns expressed under para 42 and address them in the PPS.

Appendix A – Selected Applications

Android - Selected Mobile Apps (The ranking and the numbers of installation were as at 6 May 2013)

Chart	Ranking	Category[5]	Name of App	No. of Install
Top Paid	90	Travel & Local	香港航班資訊 Pro	500 - 1,000
	157	Transport	香港小巴 Pro	100 - 500
Top Free	8	News & Magazines	蘋果日報 AppleDaily	1,000,000 - 5,000,000
	15	Communication	小熊來電通知	1,000,000 - 5,000,000
	59	Weather	香港地區天氣	500,000 - 1,000,000
	65	Lifestyle	香港六合彩 (Mark Six)	1,000,000 - 5,000,000
	92	News & Magazines	RTHK On the Go	500,000 - 1,000,000
	93	News & Magazines	無線新聞	100,000 - 500,000
	111	Entertainment	Ticketing-Broadway/PALACE/AMC	100,000 - 500,000
	112	Finance	Money18 免費即秒報價及股市資訊	100,000 - 500,000
	115	Transport	香港小巴	100,000 - 500,000
	128	Shopping	香港格價網 Price.com.hk (手機版)	100,000 - 500,000
	136	Game	3 國小豬 腦力王世紀大賽	50,000 - 100,000
	145	Finance	中銀香港	100,000 - 500,000
	153	News & Magazines	now 新聞直播	100,000 - 500,000
	155	Travel & Local	小熊流動巴士版圖	100,000 - 500,000
	173	Travel & Local	香港航班資訊	100,000 - 500,000
	174	Entertainment	商台節目重溫	10,000 - 50,000
	201	Entertainment	TVB fun	500,000 - 1,000,000
	202	Lifestyle	香港查詢	100,000 - 500,000
	219	News & Magazines	爽報香港	500,000 - 1,000,000
	245	Business	互動就業服務 iES	100,000 - 500,000
	258	Social	香港討論區	50,000 - 100,000
Top Grossing	4	Game	逆轉三國	500,000 - 1,000,000
	10	Game	逆戰幻想(Card RPG Fantasica)	100,000 - 500,000
	63	Game	龍之逆襲	100,000 - 500,000
	75	Game	海賊幻想	100,000 - 500,000
	124	Game	忍者無極 2 (Ninja Royale 2)	10,000 - 50,000
	128	Game	掌上三國	100,000 - 500,000
	203	Social	香港高登（官方版 beta）	100,000 - 500,000

[5] according to Google App Store

iPhone - Selected Mobile Apps (The ranking was as at 6 May 2013)

Chart	Ranking	Category[6]	Name of App
Top Paid	19	Travel	Hong Kong Taxi Translator
	53	Games	Mahjong World 麻將天下
	156	Travel	曼谷旅遊 Guide
	264	Games	娜娜聲，估歌仔 NaNaSing
Top Free	29	Games	神魔之塔
	55	Entertainment	myTV
	60	Food & Drink	Ippudo Passport 一風堂拉麵國通行證
	86	Food & Drink	OpenRice Hong Kong 開飯喇
	93	Travel	新巴城巴 CitybusNWFB
	104	News	i-cable.com 流動版
	117	Entertainment	UA Ticketing - UA Cinemas
	121	Games	iHorse Racing
	122	Travel	KMB & LW
	129	Travel	MTR Mobile
	133	Entertainment	Hong Kong Toolbar
	137	Utilities	one2free Playground
	149	Food & Drink	Happy McD
	155	Education	遊學世界 Flash Card
	156	Weather	MyObservatory
	165	Business	美聯物業筍盤
	167	Lifestyle	Hong Kong Movie 香港電影
	169	Lifestyle	Yahoo! HK Deals
	183	Food & Drink	Genki Sushi Online Queuing
	184	News	CABLE 即時睇
	186	Utilities	通訊事務管理局辦公室寬頻表測試 OFCA Broadband Performance Test
	194	Navigation	中原地圖 Centamap 手機版
Top Grossing	15	Games	熱血兄弟(Blood Brothers)
	49	Games	巴哈姆特之怒．霸絶蒼穹
	69	Games	大話龍將
	189	News	on.cc 東方互動- 電子 HD 版

[6] according to App Store

Appendix B – Examination of Applications

Regarding the pre-installation screens

1. Whether Chinese and/or English were used?
2. Whether PPS was available, and in what language?
3. Whether there was a labelled PPS link to a website, and whether such link links correctly to a PPS?
4. Whether there was any link to the website of the developer?
5. Whether any general/privacy-related contact details (phone, fax, email, address etc.) were available?
6. What types of smartphone data did the app want to access?

Regarding the websites of the developers

7. How easily could the PPS be found in the website? How many clicks were required to access them? What was the path to access them from the home page or the landing page from the app's pre-installation screen?
8. Whether any general/privacy-related contact details (phone, fax, email, address etc.) were available?

Regarding the PPS

9. Whether Chinese and/or English were used in the PPS?

Regarding the app

10. Whether Chinese and/or English were used in the app?
11. Whether the app required logging in using an account before it could be used?
12. Whether any in-app advertisement was shown?