A Study of Android Apps' Privacy Policies

Daniel Xiapu Luo
The Hong Kong Polytechnic University
Privacy Policy

- Explain what data will be accessed/transmitted/stored/shared/used by the app as well as the reasons.
- Emphasize what data will not be accessed/transmitted/stored/shared/used by the app.

Android version

1. The HKO will record visits to the "MyObservatory" ("the app") without collecting any personal identifiable information from users. Such general statistics are collected to compile statistical reports and diagnose problems with, or concerning, computer systems to help improve the app.

2. To provide location-based weather service, the app would get user’s location and present data that is most relevant to the user by retrieving information from servers of the HKO. User’s locations would not be transmitted out from the app. This feature requires user’s authorization on “approximate location (network-based)” and “precise location (GPS and network-based)”.

3. To allow user to gain access to HKO’s Dial-A-Weather (DAW) service, the app would call the DAW hotline when user presses DAW link in the app. The app would not access to any information in the address book of user’s smartphone. This feature requires user’s authorization on “directly call phone numbers”.

4. To reduce waiting time for downloading data after loading the app with a view to improving user experience, the app would store downloaded data on user’s smartphone. This feature requires user’s authorization on “modify or delete the contents of your USB storage”.

5. As Google map is employed for displaying data in “Storm Track”, “Lightning Location” and “Radiation Level”, the app requires user’s authorization on “read Google service configuration”.

6. The app may use camera lens of the smartphone in the “My Weather Report” feature, and save the photos taken by users on user’s smartphone. The app would not access any information in photo album of the smartphone.

7. The app supports sharing of information via third party service providers (“Share” function). If you use the “Share” function, please refer to the privacy policy of corresponding service providers.

http://m.weather.gov.hk/wxmore/my_observatory_privacy_policy.htm
California Targets Mobile Apps For Missing Privacy Policies

Mobile app developers that don't post conspicuous online and in-app privacy policies will face $2,500 fine per download.

Mobile app developers, beware: California is set to begin fining mobile app developers that release apps that lack a clear -- and easily accessible -- privacy policy.

The state's Attorney General, Kamala D. Harris, this week began notifying numerous businesses that collectively develop as many as 100 different mobile apps that they're currently breaking the California Online Privacy Protection Act -- a.k.a. CalOPPA -- by not having such privacy policies in place. In letters dated Oct. 29, the businesses were informed that they have "30 days to conspicuously post a privacy policy within their app that informs users of what personally identifiable information about them is being collected and what will be done with that private information," according to a statement released by Harris's office.

10 Best Apps For the Samsung Galaxy Note
(click image for larger view and for slideshow)
新聞

日期：2015年1月8日

2014年

資訊科技界鼎力支持推動「應用程式重私隱 創新科技贏信任」保障私隱活動

(2015年1月8日)個人資料私隱專員公署（「公署」）為流動應用程式開發商而設的保障私隱活動（「活動」）今日正式展開。

個人資料私隱專員蔣任宏表示：「推動及監察流動應用程式業務的持份者遵從《個人資料私隱條例》（「條例」）是我們2014及2015年的重點工作，鑒於公署分別在2013及2014年抽查流動應用程式，結果均發現它的私隱政策透明度明顯不足。在抽查的程式中，只有大約一半有提供相關資訊，而且大部分的私隱政策聲明都有不足之處，例如相關性低、難於閱讀及及不易查閱。再者，七成以上被抽查的程式在安裝前並沒有清楚說明會否讀取並儲存書動裝置內的去資料、哪些資料及為何讀取，八成半被抽查的程式要求讀取資料的權限與其主要功能相比，似乎超越用戶所預計的實際需要。」

公署會手持機商

是次活動以「應用程式重私隱 創新科技贏信任」為主題，由資訊科技界十個專業團體及商會協辦，並得到九個業內的專業及學術機構支持（附件一）。公署在活動期間會推出一系列的培訓活動，協助流動應用程式開發商了解及遵從他們在條例下的法律責任。

個人資

蔣任宏今日與資訊科技界立法會議員莫乃光一同主持活動的開幕儀式，他指出：「業界的大力支持讓我們非常鼓舞，公署認同業界的抱負：積極推動香港的資訊科技，以促進經濟及社會的發展。在這過程中，消費者的私隱及資料得以保障，實在是至為重要。」

為提升

蔣任宏補充：「其實把私隱保障融入資訊科技系統並不會剝奪該系統的安全性、使用、效率、操控或其他有用的功能或特性。有些說法指要保障私隱就是阻礙科技發展，魚與熊掌不可兼得，其實是誤解。相反，保障私隱能增加消費者的信心，從而締造雙贏局面。」

為提升

莫乃光表示：「隨著用戶享用流動應用程式提供的服務日趨複雜，開發商在流動裝置產生、處理及儲存的資料也愈來愈多。設計程式時顧及私隱，可讓用戶更易掌控其資料如何被讀取及使用。提高隱私方面的透明度更能樹立資訊科技界的正面形象，嬴取消費者的信任，從而令業界得益。」

公眾自去年1月已加強向程式開發商推行培訓，共舉辦了八場研發流動應用程式講座，亦在去年11月發出《開發流動應用程式最佳行事方式指引》^{2}，以協助開發商研發保障私隱的應用程式。此外，公眾透過廣告、社交媒體及專題網站^{3}，為公眾提供了簡便的指引及短片以提高他們保障網上私隱的意識。
Outline

- Checking App’s Privacy Policies *Automatically*
- Generating Privacy Policies Templates for Apps *Automatically*
- Conclusion
Common Faults in Privacy Policies

- **Incomplete privacy policy**
  - The privacy policy does not cover an app’s all behaviors of accessing personal information.

- **Example**
  - Get location information without claiming such behavior in its privacy policy.

  ```
  Description:
  Location aware tasks will help you to utilize your field force in optimum way.
  
  Class: com.dooing.dooing.ee  Method: G
  <android.location.Location: double getLatitude()>
  <android.location.Location: double getLongitude()>
  ```
Common Faults in Privacy Policies

- Incorrect privacy policy
  - An incorrect privacy policy declares that the app will not collect, use, retain, or disclose personal information, but the app does.

Malware Abuses Android Accessibility Feature to Steal Data

By Eduard Kovacs on July 03, 2015

Researchers at mobile security firm Lookout have come across a piece of malware that abuses the accessibility service in Android to steal sensitive data from infected smartphones.

The threat, detected as “AndroRATIntern” and sold commercially as “AndroidAnalyzer,” is a surveillance tool created with the AndroRAT toolkit. Lookout says it’s the first threat that abuses accessibility features offered by the Android operating system for data theft.

According to Lookout, the malware is utilized to target users in Japan. Once it’s deployed on a smartphone, the Trojan is capable of collecting contact data, SMS messages, videos, photos, call logs, GPS location, SD card changes, and messages from LINE, a popular communications app developed by a Japan-based company.
Common Faults in Privacy Policies

- **Inconsistent privacy policy**
  - The privacy policy of an app is in conflict with that of its third-party libs.

- **Example**
  - A popular game app’s privacy policy says:
    - “we do not use or collect your precise geographic location.”
  - It uses a third-party library, Unity3d, whose privacy policy says:
    - “We receive information about Users, their devices, locations and interactions with the Service primarily in two ways.”
Automatically Checking Privacy Policies

Our tool analyzed 1,197 popular apps downloaded from Google play store and found that 282 apps (i.e., **23.6%**) contain at least one kind of problem.

Incomplete Privacy Policy

- 180 questionable apps

---

**Internet technology requires some basic information in order for users of websites or mobile apps to use our online services smoothly. The basic information should include but not limited to IP addresses and/or domain names, browser type and settings, language settings, geographical district, operating system, and time/duration of visit. These data are anonymous and cannot be used to identify the user under general situations. When personal identifiable information of users are involved or collected in the Federation's websites or mobile apps, users will be prompted to give explicit alert of the collection so as to give consent.**
Incorrect Privacy Policy

- A few questionable apps.

- **Example 1**
  - **Privacy policy**
    - “we are not collecting your data of birth, phone number, name or other personal information, nor those of your contact.”
  - **Code**
    - Collect contact information.

- **Example 2**
  - **Ambiguous privacy policy**
    - “we will not store your real phone number, name and contacts”
    - “Users locations would not be transmitted out from the app”.
  - **Code**
    - They get the information and write to log file.
    - Note: third-party libs in the app or colluded apps can access the information in log file; attackers could use adb to access the log; apps in a rooted smartphone could access the log.
Inconsistent Privacy Policy

- 41 questionable apps

Example

- App’s privacy policy
  - “we do not collect information such as your real name, address, or phone number.”

- Third-party lib’s privacy policy
  - “we may collect device specific information (such as ... mobile network information including phone number)”.

Example

- App’s privacy policy
  - “We don’t share your personal information with any third parties”.

- Third-party lib’s privacy policy
  - “We may share certain types of personal information with third parties.”
Outline

- Checking App’s Privacy Policies *Automatically*
- Generating Privacy Policies Templates for Apps *Automatically*
- Conclusion
Writing Privacy Policy

- **Is it difficult?**
  - **No**, because
    - PCPD provides many guidelines and training courses.
    - Free online generators.
  - **Yes**, because the author of a privacy policy may
    - not be familiar with the precise operation of each API used.
    - not know the internals of the integrated third-party libraries.

---

---

---

---
Our tool takes in an apk file and then generate a correct and readable privacy policy template for it.

**Information Collection And Use**

While using our application, this application will collect some personal information from your device.

(*) Personally Identifiable Information Collected by This Application.
   We would access unique device ID. This information will be wrote to log.
   We would use location(including, latitude and longitude).
   If Wi-Fi is enabled, we would access mac address of wifi and IP address.
   If the device is in an interactive state, we would check running tasks.

(*) Non-Personally Identifiable Information Collected by This Application.
   If Wi-Fi is enabled, we would check network type(e.g., GPRS, HSPA, LTE, UMTS).

**Cookies**

Cookies are files with small amount of data, which may include an anonymous unique identifier. Cookie will be used by this app.

**Third Party Library and Information Disclosed to them**

The following third party libraries are used by this application: Millennial, AdWhirl, Admob(Google), Flurry Analytics.

These third party libraries will also collect some information:
   If network connectivity exists, Millennial would access unique device ID.
   AdWhirl would use location(including, latitude and longitude).
   Admob(Google) would access latitude and longitude.
   Flurry Analytics would use location(including, latitude and longitude).
Evaluation

- Comparing the coverage of the privacy policies generated by our tool and that of existing privacy policies.
  - “N”: privacy policies generated by our tool, “O”: existing privacy policies
  - Existing privacy policies may be either **incomplete** or **imprecise**.

<table>
<thead>
<tr>
<th>App Num</th>
<th>Device ID</th>
<th>Location</th>
<th>Account</th>
<th>Camera</th>
<th>Audio</th>
<th>App List</th>
<th>Cookies</th>
<th>Phone Num</th>
<th>Call log</th>
<th>Calendar</th>
<th>Lib Num</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>N O</td>
<td>N O</td>
<td>N O</td>
<td>N O</td>
<td>N O</td>
<td>N O</td>
<td>N O</td>
<td>N O</td>
<td>N O</td>
<td>N O</td>
<td>N O</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>10 9</td>
<td>8 8</td>
<td>1 1</td>
<td>7 0</td>
<td>1 0</td>
<td>4 1</td>
<td>9 9</td>
<td>2 1</td>
<td>2 0</td>
<td>1 0</td>
<td>20 4</td>
</tr>
</tbody>
</table>
Evaluation

- Readability comparison between existing privacy policies and the generated privacy policies.
- Is this privacy policy easy to read?
Evaluation

- Understandability comparison between existing privacy policies and new generated privacy policies.
- Do you think an app with such behavior violate user privacy?
Conclusion

- For normal users, please read the privacy policy before installing an app if it is available.

- For app developers, please provide clear privacy policies following the suggestions from PCPD, get familiar with the APIs/third-party libs used, and avoid over-claiming permissions.

- For companies that outsource the app development, please check the code and the privacy policy carefully before releasing the app.

- We would like to provide free services based on our tools to various users in the future if resources permit, and welcome collaborations.
Thanks my group members and collaborators for contributing to this research.

- Mr. Le Yu, Mr. Chenxiong Qian, Mr. Xule Liu, Dr. Tao Zhang, Dr. Henry Chang

Contact

- Dr. Daniel Xiapu Luo
- Department of Computing, The Hong Kong Polytechnic University
- Email: csxluo@comp.polyu.edu.hk
- https://www4.comp.polyu.edu.hk/~csxluo/