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

Information Leaflet

Personal data privacy protection: what mobile apps developers and their clients should know

Introduction

This technical information leaflet aims to highlight the privacy implications that mobile applications ("**mobile apps"**) developers (including organisations who commission the development of mobile apps) and operators (referred collectively as "**Apps Developers**") should consider in connection with designing and developing mobile apps. It suggests good privacy protection practices for Apps Developers to follow in compliance with the Personal Data (Privacy) Ordinance (**"the Ordinance"**), and in particular, the six data protection principles[1] ("**DPPs**").

What are Mobile Apps?

Mobile apps, within the context of this leaflet, refer to mobile device applications that are often capable of capturing the location information of the mobile device, accessing address book, calendar or albums, and/or support voice/multimedia communication via the Internet or the mobile telephony network. Typically this category of devices includes smartphones and tablet computers.

Mobile Apps, Personal Data and the Ordinance

Mobile devices are usually considered very personal and private as they often perform the role of personal organisers and are carried around and used by individuals. Mobile devices often are used to store information such as locations travelled, photographs taken, text messages sent and received, address book contacts entered, and social network usernames and passwords used.

Normally, Apps Developers will collect personal data by directly asking mobile device users to provide their personal data. Additionally, through mobile apps, Apps Developers may access, transfer, share or upload user-supplied or device-specific data stored in mobile devices with or without the notice of the mobile device users. Whether the information so collected is personal data, hence falling within the jurisdiction of the Ordinance must be judged on a case by case basis. The information is personal data if all of the three conditions below are satisfied:-

(a) it relates directly or indirectly to a living individual;
(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
(c) it exists in a form in which access to or processing of the information is practicable.

Privacy Risks

Apps Developers should be mindful that they often collect or access a wide range of data from which, taken together, it is possible to identify a specific individual. Furthermore, Apps Developers that collect a wide range of data may be capable of building over time an individual's profile about his/her activities, which causes privacy concern.

[1] available at http://www.pcpd.org.hk/english/ordinance/ordglance.html

Encouraged Good Practices

In view of this, the following practices on the protection of personal data, though not specified under the Ordinance, are encouraged as good practice to be followed by Apps Developers:

The Privacy by Design Approach

Apps Developers that access or share personal data in mobile devices are recommended to adopt the Privacy by Design ("**PbD**") approach (i.e. the philosophy of embedding privacy from the outset into the design specifications) when designing mobile apps. The seven principles of PbD are:-

1. Personal data protection should be proactive (not reactive) and preventative (not remedial) in nature;
2. Personal data protection should be the default setting;
3. Personal data protection should be embedded into the design of the apps and not bolted on after an app is developed;
4. PbD should not be a trade off against functionality or security, but should achieve positive-sum, win-win, outcomes;
5. Personal data protection should cover the entire cycle of personal data flow from collection to erasure;
6. PbD should be open and transparent to all stakeholders;
7. PbD should be user-centric.

Privacy Impact Assessment

A Privacy Impact Assessment ("**PIA**") is a PbD tool that can be used to systematically evaluate at an early stage the design of a process or a system (such as a mobile app) in terms of its impact upon personal data privacy with the objective of detecting any risks and avoiding or minimising any adverse impact. Although PIA is not expressly provided for under the Ordinance, it is a well-known compliance and risk assessment tool which Apps Developers are encouraged to adopt for designing and developing mobile apps.

For more information, please refer to Information Leaflet – Privacy Impact Assessment published by the Privacy Commissioner for Personal Data ("the Commissioner")[2].

Recommended Practices for Complying with the DPPs

If Apps Developers use mobile apps to collect personal data, they must comply with the requirements under the Ordinance including the six DPPs which regulate organisations (referred to as "**data users**" under the Ordinance) engaging in the collection, holding, processing and use of personal data. Below are the DPPs and the recommended practices for Apps Developers to follow.

DPP1 – Purpose and manner of collection

- The purpose(s) of collecting or transmitting personal data from/through the mobile devices must be lawful and directly related to a function or activity of the data user;
- Personal data collected must be necessary but not excessive for the collection purpose;
- Personal data must be collected in a lawful and fair manner;
- If personal data is collected directly from individuals (referred as "**data subjects**" under the Ordinance), they should be informed of whether it is obligatory or voluntary to supply the data, the purpose of uses of the data, the classes of persons to whom the data may be transferred, and the rights of the data subject to request access to and correction of the

[2] available at http://www.pcpd.org.hk/english/publications/files/PIAleaflet_e.pdf

data. This information is generally communicated in a Personal Information Collection Statement (PICS).

Personal Information Collection Statement
Apps Developers have to provide mobile device users with a PICS on or before collecting their personal data. They should communicate to the mobile device users under what circumstances will their personal data be collected, accessed or shared and for what purposes. This notice should be presented to mobile device users clearly before they confirm installing the mobile apps.

Mobile Apps Declaration
If permission to access certain data needs to be declared in the programming codes of the mobile app before the access can be granted by the mobile device, Apps Developers should make sure that the access is indeed made in the mobile app. If the permission declarations cover more gratuitous data than the mobile app uses, mobile device users who are able to spot the declared but unnecessary/unused access may doubt the intention and genuineness of the mobile apps. For example, if data subjects find in the permission page of an action game that it would access the diary of the mobile device, data subjects may question such a need and refrain from using the game even if the game never actually access any diary entries.

Permission-Model
Information stored in mobile devices is likely to be sensitive information of the mobile device users. In the interest of fairness, Apps Developers should fully inform mobile device users of the collection, access, transmission or sharing of their information. Apps Developers are also encouraged to consider a permission-based access model where permission has to be sought from the mobile device users whenever a new type of information is accessed, transmitted or shared for the first time. This is to ensure that mobile device users have actual knowledge about such access, transmission or sharing. Mobile apps should be developed to allow mobile device users to select the individual types of information to give access permission to, and behave accordingly. Furthermore, Apps Developers should consider building a configuration screen in the mobile app to show the access permissions given by the mobile device users for each type of information, and allow for subsequent giving or withdrawals of permission.

DPP2 –
Accuracy and duration of retention

- Data users must take all reasonably practicable steps to ensure the accuracy of the personal data held by them;
- All reasonably practical steps must be taken by data users to ensure that personal data is not kept longer than is necessary for the fulfilment of the purposes for which the data is used;
- If a data user engages a data processor[3] to process personal data on its behalf, the data user must adopt contractual or other means to prevent the personal data transferred to the data processor from being kept longer than is necessary for processing of the data.

Unnecessary Retention of Personal Data
To comply with the retention principle, Apps Developers should consider discarding completely information uploaded or stored in backend servers as soon as it is no longer necessary for the use of the mobile app. For example, if a new copy of the address book must first be uploaded to server each time the mobile app is to function, there should be a mechanism to erase the previously uploaded copy as soon as the use of the app is completed.

[3] Data processor means a person who processes personal data on behalf of another person, and does not process the data for any of the person's own purposes.

Removal Commitment
Account information (including uploaded or shared information) of a mobile device user should be completely removed upon the user's request or upon account termination unless there is legal or regulatory reason not to do so. Apps Developers should make this account removal function easily accessible.

Outsourcing
If outsourcing agents are engaged to develop or operate mobile apps, Apps Developers should adopt contractual or other means to require the outsourcing agents to (i) keep logs on access and use of the personal data; (ii) erase personal data under specified circumstances and intervals; (iii) use industry-standard data erasure software; (iv) timely report on the erasure actions; and (v) be subject to review and audit by the Apps Developers or an independent party.

For more information, please refer to Information Leaflet – Outsourcing the Processing of Personal Data to Data Processors[4] published by the Commissioner.

DPP3 –
Use of personal data

- Personal data shall not, without the express and voluntary consent of the data subject, be used for a purpose other than the purpose for which the data was to be used at the time of the collection of the data or a directly related purpose.

Avoidance of Function Creep
It is not uncommon that after accumulating personal data from mobile apps for some time, Apps Developers then realise the potential for use of such personal data for other purposes (such as data mining, profiling etc.). If such new purpose of use of the data is not directly related to the purpose originally communicated to device users during the collection, Apps Developers must obtain the express and voluntary consent from the mobile device users before using the data for a new purpose.

DPP4 –
Security of personal data

- Data users must take all reasonably practicable steps to protect the personal data held by them from unauthorised or accidental access, processing, erasure, loss or use;
- If a data user engages a data processor to process personal data on its behalf, the data user must adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

Software Development Tools
Trojan horses or backdoors for accessing mobile device information without authorisation may be introduced to mobile apps unknowingly if rogue software development tools are used. To avoid this, Apps Developers should use reliable and/or official versions of software development tools (e.g. software development kits, software libraries) for the development of mobile apps.

Secure Coding
In order to minimise the potential vulnerability to hacking or inadvertent data breach, Apps Developers should follow the industry best practice in secure coding to ensure the robustness of their mobile apps. Secure coding guides on specific computer languages are available from organisations such as CERT [5] . Mobile device manufacturers also publish their own secure coding guides and should be referred to for the design and development of mobile apps.

[4] available at http://www.pcpd.org.hk/english/publications/files/dataprocessors_e.df

[5] available at http://www.cert.org/secure-coding/

Encryption
All information transmitted to and from the mobile apps should be encrypted to avoid interception. If information must be kept in the backend servers, the stored information should be protected by access control and encryption to avoid unauthorised access.

Code Review and Testing
Apps Developers should perform code review and testing of the mobile apps prior to launching them, not only for the purpose of spotting bugs but also for ensuring that there is no intended or unintended access to information inconsistent with the design specifications of the mobile apps.

Outsourcing
If outsourcing agents are engaged to develop or operate mobile apps, Apps Developers should adopt contractual or other means to require the outsourcing agents (i) to use genuine (i.e. not pirated) and reliable development tools and software; (ii) to maintain formal access control on personal data by its staff; (iii) to report promptly any data breach; (iv) to be subject to review and audit by the Apps Developers or an independent party; and (v) not to sub-contract or further outsource the work unless the same level of protection can be assured.

For more information, please refer to Information Leaflet – Outsourcing the Processing of Personal Data to Data Processors mentioned above.

DPP5 –
Information to be generally available

- Data users must take all reasonably practicable steps to make available to anyone their personal data privacy policies and practices, including the kinds of personal data held by them and the purpose for which the data is to be used.

Privacy Policy Statement (PPS)
Apps Developers should prepare a PPS to outline their policies and practices in relation to personal data. Technical terms and elusive language should be avoided in the PPS. It should be easily readable and easily understandable, and in appropriate length. Its location on the mobile apps should be prominent. Its availability also on the businesses' normal websites is recommended.

Giving examples in PPS
When describing the purposes for which the information is to be used in the PPS, Apps Developers should consider giving real-case examples (as opposed to generic statements) specific to the mobile apps to assist mobile device users in understanding why such information needs to be collected, accessed or shared.

Relevance and Accuracy
Apps Developers should ensure that their PPS are accurate and specific for individual mobile apps. If the description is vague or unclear, the Apps Developers may be perceived as hiding the real purpose of data collection and access. Similarly, if the PPS is copied or extracted from a standard template or another mobile app, Apps Developers have to review the contents to ensure their relevance and accuracy.

DPP6 –
Access to personal data

- A data subject is entitled to ascertain from a data user whether it holds his/her personal data and to obtain a copy of the personal data. He/She can also request the correction of the personal data.

Contact Details for Making Data Access and Correction Requests

Apps Developers should make available their contact details (including name or post title, and address) in the mobile apps to facilitate mobile device users to make data access and correction requests. They should also have policies and procedures in place to ensure that a request is complied with or refused (as the case may be) within 40 days from receiving the request. Please refer to the Guidance on the Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users published by the Commissioner[6].

Apps Developers are Responsible for their Compliance

The advice and recommendations above are not meant to be exhaustive nor do they represent building blocks of a fully compliant mobile app model. Different mobile apps have different characteristics and functions. Apps Developers have to exercise due care and diligence to explore and adopt the most suitable ways of protecting personal data, and compliance with the Ordinance.

[6] available at http://www.pcpd.org.hk/english/publications/files/DAR_e.pdf

Office of the Privacy Commissioner for Personal Data, Hong Kong
Enquiry Hotline: (852) 2827 2827
Fax: (852) 2877 7026
Address: 12/F, 248 Queen's Road East, Wanchai, Hong Kong
Website:www.pcpd.org.hk
Email: enquiry@pcpd.org.hk