What's Up with Apps in Hong Kong
July 2013

In May this year, the Hong Kong Privacy Commissioner for Personal Data ("Privacy Commissioner") joined the Global Privacy Enforcement Network ("GPEN") to conduct a privacy review to evaluate the transparency in the collection and use of personal data online by corporate data users, with a focus on information collected via software applications ("Apps"). This review highlights the rising concern of data privacy enforcement authorities and the public on the collection and use of personal data by App providers, both in Hong Kong and worldwide.

In November 2012, the Privacy Commissioner issued an information leaflet, "Personal data privacy protection: what mobile apps developers and their clients should know" (the "Privacy Information Leaflet", which can be accessed here), to provide App developers and users with practical guidance on how to comply with the Personal Data (Privacy) Ordinance Cap. 486 ("PDPO").

In this article we discuss the review being carried out by the Privacy Commissioner and highlight the major recommendations made in the Information Leaflet, and highlight some of the direct marketing issues to be taken into account in light of the recently enacted Personal Data (Privacy) Amendment Ordinance ("Amendment Ordinance"). Our newsflash regarding the Amendment Ordinance can be accessed here.

APPS ON THE RADAR

Apps are a great way for organisations across a multitude of industries to promote and market their businesses. However, due to events over the last year, concerns regarding data privacy in respect of Apps are on the rise.

In a survey commissioned by the Privacy Commissioner on or around November 2012, it was found that less than half of the App users being surveyed knew what personal data on their phones was being accessed through the Apps installed on their devices, e.g. by the App developers, including those who commissioned and/or operate the App.

INTERNET PRIVACY SWEEP

The Privacy Commissioner conducted an Internet Privacy Sweep in Hong Kong from 6 to 12 May 2013, along with other members of the GPEN across the globe. The GPEN consists of nineteen privacy enforcement authorities from around the world (including the Privacy Commissioner, and privacy enforcement authorities in the UK, Australia and the US). This is the first annual international Internet Privacy Sweep being conducted by members of the GPEN. The aim of the Internet Privacy Sweep is to increase awareness of privacy rights and responsibilities, both by the public and organisations; to identify privacy concerns that need to be addressed; and to encourage compliance with the local privacy laws.

As part of the Internet Privacy Sweep, the Privacy Commissioner examined the availability, clarity and accessibility of privacy policies and Personal Information Collection Statement ("PICS") that local Apps provide to users upon installation of the Apps.

The results of the Internet Privacy Sweep will be announced by the Privacy Commissioner in July/August this year, and may lead to follow up actions being taken by the Privacy Commissioner, such as the issuance of enforcement notices.

PRIVACY INFORMATION LEAFLET

Apps usually collect a significant amount of data about their users or require access to data stored on a user's phone, e.g. accessing calendars, UDIDs, address books, photo albums, etc. The collection of such a wide range of data may, collectively, make it possible to identify an individual, and would therefore constitute personal data that is subject to the protection of the PDPO.

It is essential for App developers (including those who commission the development of an App) ("App Developers") to be open and transparent about what personal information will be collected and used, in a way which can be easily understood by users and provided on or before the time of collection, to enable users to make an informed decision.

www.hoganlovells.com
The Privacy Information Leaflet provides practical guidance to App Developers to ensure compliance with the PDPO. Whilst some of the guidance in the Privacy Information Leaflet is not specifically required under the PDPO, compliance with it is still encouraged as a matter of good practice. Further, any non-compliance with the Privacy Information Leaflet may be used by the Privacy Commissioner against an App Developer in its investigation into any alleged breach of the PDPO.

Building Privacy into the Design of the App

App Developers should adopt the approach of embedding privacy into the App's design specifications right from the outset (i.e. a “Privacy by Design” approach), whereby the following principles should be applied:

(a) a proactive and preventative data protection approach should be adopted;
(b) the default position should be personal data protection;
(c) personal data protection should be embedded in the App's design, and not bolted on after the App has been developed;
(d) there should not be a trade-off between privacy, security and functionality;
(e) personal data protection should cover personal data from the time of collection to erasure;
(f) the protection should be open and transparent; and
(g) it should be user-centric.

The Privacy Commissioner also recommends that a privacy impact assessment be carried out to evaluate the design of the App to determine any risks in relation to data privacy, and to assess how to such risks can be minimised and avoided.

Personal Information Collection Statement

Personal data of a user should only be collected by the App Developer to the extent necessary in order for the user to be able to use the App, or any other purpose consented to by the user. The personal data must also be collected in a manner that is lawful and fair, and the purpose for collection must be directly related to a function or activity of the App Developer.

Under the PDPO, App Developers must inform users of the following on or before the time of collection of his/her personal data (e.g. prior to the user's installation of the App onto his/her mobile phone): (i) whether it is obligatory or voluntary for users to provide the personal data, and the consequences of failing to do so; (ii) the purpose of collection of the data; (iii) the classes of persons to whom the data may be transferred to; and (iv) details about the user's right to request access to and correction of his/her data. The Privacy Information Leaflet recommends that the above information be set out in a personal information collection statement ("PICS").

The PICS must clearly set out the circumstances in which personal data of a user will be collected, accessed or shared (i.e. what type of data will be collected, accessed or shared) and for what purpose. The PICS must be clearly presented to the users before they agree to install the App on their mobile device. For example, upon clicking the “install” button in the App Store, a message may appear on the screen containing the PICS, which the user must confirm acceptance of by clicking a button, before it can proceed with the installation of the App.

Any new use of personal data by the App Developer, that is not directly related to the purpose originally communicated to the users upon collection (e.g. under the PICS), must be expressly and voluntarily consented to by the user before the App Developer may use the data for such new purpose. App Developers are recommended under the Privacy Information Leaflet to consider incorporating a permission-based access model, whereby permission must be obtained from the user whenever the App Developer wishes to access, transmit or share for the first time a new type of information not covered in the PICS. This will ensure that users will have actual knowledge about the type of data being accessed, used or transmitted. The App should be developed to enable users to choose the type of personal data that the App Developer can have access to, and for the App to only access, use or transmit data in accordance with such permission. For example, if a user accesses a new feature of an App that will require the collection of, say, the user's address book, the App should have a pop up notice notifying the user (before the information is collected), amongst other things, that such information will be collected, the purpose for such collection and any third parties that the information may be transferred to. The user may then provide its consent for such collection by clicking a button.

Unnecessary Retention of Personal Data

Under the PDPO, App Developers are required to take all practical steps to ensure that personal data of a user is not kept longer than is necessary for the fulfilment of the purposes for which the data is used. The Privacy Information Leaflet recommends that App Developers consider completely deleting information uploaded or stored in its back-end servers as soon as it is no longer necessary for the use of the App. For example, if the current location of a user must first
be uploaded to the server each time the App is to function, there should be a mechanism in place to erase the previously uploaded location information of the user as soon as the use of the App is complete.

The Privacy Information Leaflet also advises that any account information of a user (including uploaded or shared information) should be completely removed by the App Developer upon the user's request or his/her termination of his/her account, unless there is a legal or regulatory reason not to do so. Such an account removal function should be easily accessible, e.g. including "delete" buttons in appropriate locations on the App.

**Security of App**

Pursuant to the PDPO, App Developers must ensure that they take all reasonably practicable steps to protect the personal data of users being held by them, so that there is no unauthorised or accidental loss, access, processing, erasure or use of the personal data.

For example, the Privacy Information Leaflet advises App Developers to only use reliable or official versions of software development tools to develop their Apps in order to avoid any "Trojan horses" or "backdoor" codes being unknowingly introduced into the Apps, which may access a user's device without authorisation. App Developers should also follow best industry practices in secure coding, and ensure all information transmitted to and from their Apps or stored on backend servers are encrypted and protected by access control to avoid any unauthorised interception or access.

Prior to the launch of an App, App Developers should perform a code review and testing of their App to ensure that the App does not access any information of a user that is inconsistent with its design specifications.

**Privacy Policy Statement**

Under the PDPO, App Developers are required to take all reasonably practicable steps to make their personal data privacy policies and practices generally available (including information on the type of personal data held by them and the purposes for which the data will be used).

The Privacy Information Leaflet advises App Developers to have in place a privacy policy statement that outlines their personal data policies and practices. It must be easily readable and understandable by the user, and of an appropriate length. Technical and elusive language should not be used, and App Developers should give real-case examples in relation to the App, to help users understand how their personal data will be used and why such information needs to be collected or shared.

The privacy policy statement should also be located on the App in a prominent place. For example, a link to the privacy policy statement could be included at the bottom of the main page of the App. It is also recommended that the privacy policy statement also be included on the App Developers normal website.

Often App Developers simply apply their privacy policies for their general websites to their Apps. However, such website privacy policies may not be relevant or accurate in respect of the type of personal data being collected, shared or used by the Apps, and may not be sufficient to comply with the PDPO. A privacy policy statement should be developed by an App Developer which is accurate and specific for each individual App.

**Users' Access**

Users are entitled, under the PDPO, to find out from an organisation (e.g. an App Developer) whether it holds his/her personal data, to obtain a copy of such data, and to request the correction of his/her data held by it.

Apps should include the contact details of the App Developer (including the name or title of the relevant individual to contact), in order to facilitate a user to make a data access or correction request. The App Developer is also advised by the Privacy Information Leaflet to have in place a procedure to ensure that any data access or correction request is complied with (or refused, as applicable) within 40 days from receipt of the request.

**Third Party Processor**

The PDPO specifically requires any data user who engages a data processor (i.e. a person who processes personal data on behalf of another and not for its own purposes), to adopt contractual or other means to prevent any personal data transferred to the data processor from: (i) any unauthorised or accidental access, loss, erasure or processing; or (ii) being kept longer than is necessary for the processing of it.
In the event that any third party is engaged by a company to develop or operate an App, the Privacy Information Leaflet requires contractual or other means to be adopted in order to require such third parties to:

(a) keep logs on access and use of personal data;
(b) erase personal data under specified circumstances and intervals;
(c) use industry-standard data erasure software;
(d) provide a timely report on the erasure actions taken;
(e) use genuine (i.e. not counterfeit) and reliable development tools and software;
(f) maintain formal access control on personal data by its staff;
(g) promptly report any data privacy breaches to the App Developer;
(h) not further sub-contract or further outsource the work unless the same level protection can be assured; and
(i) enable the App Developer or an independent party to conduct a review and audit of that third party.

App Developers should also refer to the "Information Leaflet: Outsourcing the Processing of Personal Data to Data Processors", published by the Privacy Commissioner on 27 September 2012 (available here).

DIRECT MARKETING

In the event that an App Developer intends to use any personal data of a user to provide direct marketing materials, e.g. to advertise a new App via push notifications, or to transfer any personal data to a third party for that third party to use the data for direct marketing purposes, then it must comply with the new direct marketing requirements under the PDPO.

As of 1 April 2013, the PDPO requires App Developers to provide the following additional notification to its App users before using personal data for direct marketing:

(a) a notice of their intention to use the user's personal data for direct marketing purposes (and that they cannot do so without consent);
(b) the types of personal data that will be used for direct marketing purposes;
(c) the categories of goods/services that may be marketed; and
(d) if the personal data may be transferred to a third party for direct marketing purpose, the following must be provided in writing:
1. notice of their intention to transfer the personal data for direct marketing purposes (and that they cannot do so without his/her consent);
2. the type of personal data to be transferred;
3. the classes of transferees;
4. the categories of goods and services that may be marketed by the transferees; and
5. the fact that the data will be sold or otherwise transferred for gain (if applicable).

The foregoing notification will usually be contained in the PICS. The users must be given a way of either opting-in or opting out of such direct marketing activities, e.g. a tick box in the PICS for data subjects to click on if they wish to opt-out of direct marketing. It should be noted that silence / non-response from a user does not constitute sufficient consent.

For further details regarding the new direct marketing requirements, please see our Newsflash on the new guidance on direct marketing issued by the Privacy Commissioner, which may be accessed here.

Many OS vendors prohibit the practice of sending push notifications for advertising or promotional purposes.

IMPLICATION FOR APP DEVELOPERS

Breach of the direct marketing provisions in the PDPO constitutes an offence, which may result in a maximum fine of HK$500,000 and 3 years imprisonment. Where the App Developer has sold (or otherwise transferred for gain) the personal data of a user to a third party for direct marketing purposes, in contravention of the PDPO, the maximum fine is increased to HK$1,000,000 and 5 years imprisonment.

Non-compliance with the Privacy Information Leaflet does not of itself constitute an offence, but breach of the data protection principles of the PDPO upon which the Privacy Information Leaflet is based upon may result in an investigation by the Privacy Commissioner (either commenced on its own initiative or as a result of a complaint filed with the Privacy Commissioner). If after the investigation the App Developer is found to have breached the PDPO, the Privacy Commissioner may issue an enforcement notice requiring certain remedial action to be taken. Any breach of an enforcement notice will constitute an offence. Non-compliance with the Privacy Information Leaflet may be used by the Privacy Commissioner as evidence against an App
Developer of breach of the PDPO in the event of an investigation.

Following the amendments to the PDPO which took effect on 1 October 2012, the Privacy Commissioner is now empowered to issue an enforcement notice where a contravention has been found, irrespective of whether there is evidence indicating that the contravention is continuing or is likely to be repeated. The Privacy Commissioner has been active recently in using these enhanced powers. The fact that the Privacy Commissioner issued an information leaflet providing guidance specifically relating to Apps, and has just completed the Internet Privacy Sweep with a focus on Apps, is a likely indication that he intends to pay close attention to this area in the future.

App Developers are advised to conduct a comprehensive review of their data protection policies, procedures and practices to determine whether they comply with the requirements set out in the Privacy Information Leaflet and the new direct marketing requirements in the PDPO (e.g. revising personal information collection statements, retention policies, security measures, direct marketing activities, etc.).

Contacts

Gabriela Kennedy
Partner
+852 2840 5084
gabriela.kennedy@hoganlovells.com

Karen Lee
Associate
+852 2840 5081
karenhk.lee@hoganlovells.com