Developing mobile apps — how to be privacy savvy

Davinia Brennan, Associate in the Litigation and Dispute Resolution department at A&L Goodbody, discusses the privacy risks associated with mobile apps, and the key issues which app developers should consider during the development cycle in order to comply with data protection law and protect users' privacy

In recent years, there has been an explosion of apps, with 1,600 new apps reportedly being added to app stores daily. These apps are most commonly downloaded on smart mobile devices, such as smartphones and tablets. With the increasing popularity, there has been a corresponding increase in privacy concerns amongst consumers.

According to a recent survey by the Information Commissioner's Office ('ICO') in the UK, 62% of people who downloaded an app expressed concern about the way their personal information collected through the app can be used. Almost half of app users (49%) claimed they had refrained from downloading an app due to privacy concerns.

Personal data processed by apps

The Data Protection Acts 1988 and 2003 ('the DPAs') apply in any case where the use of apps on smart devices involves processing personal data of individuals. As readers will be aware, 'personal data' are defined in the DPAs as meaning 'data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller'.

Examples of personal data processed by apps include unique device and customer identifiers (such as IMEI and mobile phone number), contacts, location data, phone call logs, SMS or instant messaging, browsing history, email content, pictures and videos, and credit card and payment data.

The app developer, being the entity that determines the purposes and means of processing personal data on smart devices, is the 'data controller', and is responsible for complying with the DPAs. However, an app developer's responsibilities will be limited if no personal data are processed or made available outside of the device, or in circumstances where the app developer has taken appropriate technical and organisational measures to ensure that data are irreversibly anonymised on the device itself, before processing the data.

Privacy obligations

The DPAs require data to be obtained and processed fairly. Personal data will not be treated as processed fairly unless app users are clearly informed of the identity of the organisation who will be processing their data, the types of personal data which will be collected if they install and use the app, the purpose for which such data will be processed, and any third parties with whom their data will be shared. The more information made available to users on how an app works, the better informed users will be. This in turn should, logically, lead to more consumer confidence in the particular app, making it more likely to be downloaded.

Only the minimum data necessary for the tasks which the app is to perform should be collected. For example, with regard to a social media app which can upload existing images from a mobile device to a central server, the app developer should ensure that, by default, the app does not collect unnecessary metadata, such as the date or location of the image, before each image is uploaded.

App developers must ensure that the data are retained for no longer than is necessary, and that appropriate security measures are taken to protect the data from unauthorised access, loss or disclosure. Users should also be able to exercise their right of access to their personal data, and to withdraw consent and delete their data or account if they so wish.

In addition, where an app developer gains access to information that is stored on the device, the consent requirement in the EC (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011, S.I. 336/2011, ('the e-Privacy Regulations') applies. Regulation 5(3) provides that information, not just personal data, may not be stored on or retrieved from a person's terminal equipment (such as a smart mobile device) unless the individual:

- has been given clear and comprehensive information about why this is being done; and
- has given his/her consent.

Accordingly, two types of consent are required from users:

- consent (or another legal ground) for the processing of the personal data; and
- consent to the placing of any information on and reading any information from the device.

Though based on a different legal basis, the two types of consent can be merged in practice, provided the user is clearly informed of what he is consenting to.

It is important for app developers to be aware that the obligation to obtain consent cannot be excluded by contractual agreement.

Compliance challenges

The small screens of smart mobile devices can make it difficult for app developers to communicate information effectively to app users. It would not be desirable or convenient to present users with a large and complex privacy policy, particularly as the average user downloads multiple apps, and expects to be able to do so quickly.

There is, in fact, no legal requirement for privacy information to be contained in one large document. Neither the DPAs nor the e-Privacy Regulations prescribe how the information is to be provided or consent is to be obtained, other than that the information must be prominently displayed and easily accessible, and as user-friendly as possible. It is vital however, that privacy information is communicated to users as soon as practicable, and before the app processes the relevant personal data.

Sanctions

Failure to comply with the DPAs can result in prosecution with a possible penalty of up to €100,000 and/or deletion of any/all data collected. In addition, section 7 of the DPAs gives a person a right to take civil action if that person suffers loss or damage as a result of the manner in which their personal data have been processed. Failure to comply with the consent requirement in the e-Privacy Regulations can also result in prosecution with a penalty of a class A fine (i.e. €5,000). Furthermore, pursuant to Regulation 16(2), a person who suffers loss and damage as a result of a failure to comply with the e-Privacy Regulations can take a civil action for that loss and damage.

Working Party Opinion

In February 2013, the Article 29 Working Party released its Opinion 2/2013 on apps on smart devices (copy available at www.pdp.ie/docs/10024). The Opinion is primarily aimed at app developers, on the basis that they have the greatest control over the precise manner in which the processing is undertaken or information presented within the app, but it also provides non-binding recommendations for other third parties involved in the development, distribution and operation of apps.

The Opinion identifies the key data protection risks to users within the app environment as including:

- a lack of transparency and awareness of the types of processing that an app may undertake;
- lack of free and informed consent from users before such processing occurs;
- poor security measures; and
- the collection of excessive personal data for an elasticity of purposes, and disregard for the principles (contained in the Data Protection Directive 95/46/EC) of 'purpose limitation' and 'data minimisation'.

The Opinion highlights the high risk to data protection flowing from the degree of fragmentation between the many players in the app development landscape, including: app developers; app owners; app stores; operating system and device manufacturers; and other third parties. According to the Opinion, it is necessary for every app to have a single point of contact who takes responsibility for all the data processing that occurs via the app. The Opinion emphasises the importance of app developers collaborating with the other parties in the app ecosystem. For example, app developers should collaborate with app stores, who can help ensure adequate information about an app, including the types of data that the app is able to process, and for what purposes, is delivered to the end user (i.e. by displaying the information in the app store catalogue).

The Opinion advocates the principle of 'privacy by design', which requires data protection to be embedded into the design of an app from the very beginning. It recommends an operating system which enables users to give a granular consent for each type of data the app intends to access. This would allow app developers to clearly inform users about the types of personal data being processed, and to obtain specific consent for each type of processing.

Guidance from the UK regulator

On 19th December 2013, the ICO released guidance to assist mobile app developers to comply with data protection law and guarantee users' privacy. It also recommends a 'privacy by design' approach to app development. It contains a useful checklist of questions for app developers to consider, including:

- will your app deal with personal data?
- who will control the personal data?
- what data will you collect?
- how will you inform your users and gain consent?
- how will you give your users feedback and control?
- how will you keep the data secure; and
- how will you test and maintain your app?

The guidance suggests the use of 'just-in-time' notifications, where

(Continued on page 7)

Examples of good (and poor) practice — from Appendix 1 of the ICO's 'Privacy in mobile apps' guide, December 2013

Example: An app allows users to record data about fitness activities, such as running or cycling, including location, altitude, speed and heartbeat. The data can be uploaded to a cloud service to share with other users of the app. The app also allows users to link with a range of popular social networking sites and automatically post updates of their most recent activities.

Good practice

There is a map on the home screen of the app with a clear marker showing the current location. This makes it clear that geo-location services are accessing the current location.

An icon is visible indicating the geo-location services of the device are active.

A clear, recognisable icon is used for the 'start' button, which must be pressed to start recording data.

A clear indication is given of which external sites the user can upload the data to at the end of the activity. There is no obligation to upload anything.

A simple means is given to access the settings to configure or to view current permissions

A simple interface is provided to remove or hide uploaded activities which the user no longer wants public.

When uploading location data, the app allows the user to 'blur' the location by, for instance, only naming the nearest town.

A simple means is provided to immediately and irretrievably delete activities the user no longer wishes to keep (e.g. a delete button next to each activity in a 'history' tab) before uploading of activities, a confirmation dialog is displayed and a progress bar is displayed with a 'cancel' option.

Where multiple reminders may cause an interruption to the user experience, an option to 'remember this option' is used with the option to disable found in the settings page.

Poor practice

Users are forced or not given an easy option to use the app without linking with a social networking site and automatically posting their recent activity.

There is no clear explanation of which sites the user's data will be uploaded to.

On first run, the app requests the user to enable public sharing of all fitness activity via a full screen notification, but the setting to disable the same feature is hidden and hard to find within the app.

Shared activities always include precise GPS co-ordinates, with no option to disable this behaviour.

Unique device identifiers (e.g. IMEI) are embedded within or otherwise linked to the fitness activities stored or uploaded to external sites.

On install, the app states that it needs permission to send SMS messages, but there is no explanation as to why this is necessary.

Users are forced or not given an easy option to use the app without granting access to stored contacts (either on the device or in social networking sites).

The app automatically sends notifications to each contact as a form of viral marketing.

The app uses Bluetooth to communicate with the user's heart rate monitor. However, the app automatically tries to pair with any nearby device and does not give the user an option to restrict Bluetooth pairing.

(Continued from page 5)

particularly intrusive data, such as GPS location, are collected. Such pop-up notifications provide the necessary information to the app user just before data processing occurs. This ensures that a user is clearly and comprehensively informed before the information is collected.

The guidance also provides examples of good and bad practice, using the example of a very popular type of app, which allows users to record data about fitness activities, such as running or cycling. These apps commonly collect personal data such as location, speed and distance data, and enable users to share this data on a range of social networking sites.

One example of bad practice includes users not being given an easy option to use the app without linking with a social networking site and automatically posting their recent activity. Other examples are reproduced on page 6.

Top ten tips for app developers

- Adopt a 'privacy by design approach' — ensure users' privacy is considered from the beginning rather than as an afterthought;
- carry out a Privacy Impact Assessment when planning an app;
- collect and process only the minimum data necessary for the task you want your app to perform (even if data are anonymised or user consent obtained);
- fully inform potential users, before their personal data are processed, of the type of data collected and the purpose of such collection (for example, via an app store or via a link to a privacy policy);
- use 'just in time' notifications for collection of more intrusive data (for example, location data);
- inform users of any third parties, such as advertising organisations, with whom their personal data will be shared;
- make provision for users to delete their personal data and any account;
- retain personal data only for as long as is necessary for the purpose for which they were obtained;
- ensure the app's default settings render it compliant with the DPAs; and
- review privacy policies regularly, and update them when necessary, to reflect any changes in the way the app processes personal data.

Conclusion

With an average smartphone user reportedly downloading 37 apps, users are inevitably becoming more privacy savvy. In order to comply with data protection law, it would be prudent for app developers to adopt a 'privacy by design' approach when developing apps. Such an approach will ensure protection of users' privacy without diminishing the functionality of the app. In addition, the provision of privacy information in a user-friendly manner will promote consumer trust and confidence and make apps more likely to be downloaded.

Davinia Brennan
A&L Goodbody
dbrennan@algoodbody.com