Apps and privacy: App-lying the rules and App-easing the users

In the first of a series of articles examining data protection and privacy issues associated with software applications, Olivia Whitcroft, Principal of OBEP, discusses the extent of data collected by apps and how to ensure consumers understand how their data are being used

During the recent Christmas break, my Android smartphone notified me that there was a brand new version of the Facebook application available. My general view is that it is good to have the latest features and bug fixes for my apps, so I selected 'Update'. As usual, I was then presented with a list of 'App Permissions', which included the following:

'NEW: Read SMS or MMS.

NEW: Add or modify calendar events and send email to guests without owners' knowledge, read calendar events plus confidential information…

Modify/delete SD card contents.'

This sounded outrageous! Why would I want Facebook to read all my text messages? I certainly did not want emails sent without my knowledge, or confidential information leaked. And what if they deleted all the photos on my SD card?

Giving myself a few moments to calm down (and finish my mince pie) before I rang the privacy police, I was led to considering possible explanations. Were these, in fact, justified actions associated with useful facilities which Facebook provides, being described 'concisely' for presentation on my mobile screen?

I therefore investigated further and found a Facebook webpage for people just like me: 'Why is the Facebook app requesting permission to access features on my Android?' It went on to explain that if I added a phone number to my account, Facebook could confirm that phone number by reading a text message that it sends to me. It also has features to allow me to see Facebook events in my phone's calendar and show my calendar availability when viewing an event on Facebook. Whilst I was still not completely clear on all elements, this sounded more reasonable and much narrower than the activities that could be inferred from the 'App Permissions'.

My next step was to go to my Facebook 'Privacy Settings' in order to investigate whether these features were present on my phone and whether options were available to enable or disable them.

As this example demonstrates, applications may collect, access and use a wide range of information in order to provide users with features, as well as allowing the provider to conduct its own analysis and other activities. Assessing the extent to which such data processing is permitted, and ensuring users understand what is going on, can be very tricky. Not all application providers are as advanced as Facebook in their evaluation of privacy issues, and not everyone will go to the trouble that I did to try to understand.

A survey commissioned by the UK regulator (the Information Commissioner's Office or 'ICO') in December 2013 produced some interesting statistics. 49% of app users who were surveyed have chosen not to download an app due to privacy concerns, and 61% are concerned about the way apps use personal information. 61% rarely or never read the privacy information when downloading a new app. These highlight the need for app developers to do more in protecting privacy and assuring consumers that they are doing so.

Difficulties in applying the legal requirements

Data protection law requires that an organisation that collects and uses data about individuals identifies fair purposes of doing so, and ensures that the data it collects and uses are relevant to, and not excessive for, such purposes. Further, the organisation should let those individuals know that such data are being used and why they are being used. Seeking specific consents or providing options to activate or de-activate features may be required for uses of data which do not directly relate to the key functions of the application.

To take a simple example, if the purpose of an app is to assist a user in finding a nearby attraction, it may need to access information about that user's location. Only such location data as is needed to find an attraction should be collected. The app should inform the user that it needs to access this data in order to provide the facility,

(Continued on page 4)

(Continued from page 3)

and how it does so in practice. The user can decide not to download the app if he is concerned. Provided the application provider makes no further use of the information, additional consents are unlikely to be required.

Unfortunately, the ease of data collection associated with software applications, and the actual or perceived value of having a large databank of information about users, has made it less likely that data processing is, in practice, kept to the minimum necessary for core purposes of an application.

Frequently, information is either requested or automatically collected, where either it is not strictly needed, or it is not obvious why and how it will be used. In addition, the app may need to treat its data processing differently depending on which device and operating system is being used to run it.

Leading on from this, the complexity of data use has made it more difficult to explain clearly to users how data are used. This is exacerbated by the culture of apps; each user wants multiple applications on each device which he can download and use as quickly as possible, and he does not want to spend time reading lengthy privacy policies and considering complex data options for each one on a small screen.

To use the example introduced above, in addition to assisting the user to locate nearby attractions, the application provider may want to keep a record of who subsequently visited a recommended place, in order to demonstrate the value of its app to other parties. However, without careful application of data protection rules (including consideration of clear notices, options and anonymisation), such further use could be unlawful.

"To use the example introduced above, in addition to assisting the user to locate nearby attractions, the application provider may want to keep a record of who subsequently visited a recommended place, in order to demonstrate the value of its app to other parties. However, without careful application of data protection rules (including consideration of clear notices, options and anonymisation), such further use could be unlawful."

Guidance from the UK regulator

On 19th December 2013, the ICO published guidance on privacy issues for mobile applications. It is stated as being aimed at app developers, but is useful reading for anyone involved in designing, creating or providing apps, or using the associated data.

The guidance recommends a 'privacy by design' approach, meaning that privacy and data protection issues be considered at the time the app is being developed, rather than as an afterthought. A Privacy Impact Assessment may be useful to assess the technology and proposed use of data and potential impact on individuals.

On the issues outlined above, the guidance emphasises that the minimum data necessary for tasks performed by the app should be collected, and that obtaining data just in case it is needed in future is bad practice, even where the user has consented.

Users must be properly informed about what will happen to their personal data if they install and use the app, and this information should be provided before the relevant data are processed.

The guidance provides practical examples of good and bad practice, including when users may need to be given clear options as to how their data are used.

Some of the ICO's suggestions and examples are discussed further below.

Defining purposes and extent of data collection

For each piece of information collected about users, app providers need to consider why they need it and how it will be used. Data may be accessed and obtained from different sources, some obvious and some less obvious (to both the user and the app provider). For example:

- details inputted by the user upon registration or on using the app, such as username, password, phone number, email address, payment details;
- information obtained from the device, such as IMEI number, location data, contact details, text and photos stored on the device (which may vary depending on the device being used);
- data generated by the application, such as user IDs, logs of use and outputs of the app's functions; and
- details obtained from linked applications, such as Google or Facebook accounts.

The importance of each data type to the aims of the app should be balanced against the risks associated with its use or misuse. In order to do this, the purposes of collection must be clearly defined, for example:

- the main functions of the app, e.g. to provide the user with a particular service;

- additional 'optional' features of the app, i.e. functions which are not required for the basic service, but may provide the user with additional benefits;
- additional actions undertaken by the app provider, e.g. data analysis, product improvement, marketing; and
- sharing data with third parties, e.g. selling contact details or sharing results of data analysis.

Where the proposed use of data is necessary for the app to perform its core functions, this is likely to be a 'fair' purpose, although this should not be assumed. Innovative apps may benefit users but still have an unjustified negative impact on their privacy. As the purposes expand into actions which benefit only the app provider or a third party, a more careful assessment may be needed to ensure that the proposed use does not unfairly or unlawfully impact the privacy of the user. Where possible, data should be processed in an anonymised form, particularly if being shared with third parties (discussed further in the next article in this series).

As highlighted by the survey referred to above, almost half of app users choose not to download an app due to privacy concerns. Aside from legal considerations, the less intrusive the app, the more likely that it may be downloaded.

Considerations and conclusions, including justifications for collection and use of each data type for each identified purpose, should be documented.

There is often misunderstanding over the extent to which obtaining a user's consent can validate additional uses of data. Whilst obtaining consent may be required or recommended for some of the identified purposes (see next section below), consent does not justify collection or use of irrelevant data. If the data are excessive for identified fair purposes, then obtaining consent does not stop the processing from being excessive and therefore unlawful. For example, if an app used to locate nearby attractions asks for consent to use national insurance number for this purpose, too much data are being requested regardless of whether consent is given.

In order to perform some functions, the app may need access to a collection of data to retrieve only certain pieces of data from that collection. The app provider should seek ways to reduce the potential negative privacy impact. Referring back to the examples given above: if Facebook needs access to my text messages in order to find one particular text message which it has sent to me, it could limit its use of information to that one text message. It does not need to read or store all of them. Similarly, if an app requires location data to find nearby attractions, knowing the general vicinity may be sufficient, and precise GPS co-ordinates (use of which is more privacy-intrusive) may not be needed.

The ICO's guidance suggests that a user's device could use GPS co-ordinates to determine the nearest town, and then only the name of the nearest town need be sent to the app's servers to work out local attractions. (Presumably this assumes that the device has another resource to determine nearby towns.)

In other words, even if a wide source of data is made available, ways to reduce the processing of those data should be explored. Unfortunately this could, in turn, reduce the benefit of the app, and it will be a matter of achieving an appropriate balance between the privacy risks and other benefits. For example, knowledge of a more precise location could improve the services provided by the app described above. The app provider may wish to consider an optional 'enhanced' service where GPS co-ordinates are collected. Users should be clearly informed of the additional privacy risks associated with the additional features (see below).

It is also worth noting that the assessment of data categories and purposes needs to include data stored or processed by any service providers on behalf of the application provider. The provider remains responsible for the actions of its service providers and cannot, for example, justify excessive data collection by asking a third party to manage such data. Having said that, making the most of a third party's expertise in handling or securing certain types of data could assist with overall privacy and data protection concerns. This will be examined further in the next article in this series.

Privacy notices and options for users

App users must be provided with clear information about how their data will be used, and any options they have to allow or disallow particular activities. As noted above, it can be very difficult to communicate in such a way that users will read and understand. The timing, wording used and method of presenting information must be carefully considered in the context of the specific app.

Timing: The law requires that, so far as is practicable, information be provided or made readily available to the individual by the time the relevant data are processed. Ideally, therefore, it should be provided before the app is downloaded, for example within the appstore. If the notice is contained within the app itself after download, the provider should not collect or make use of data until the notice has been first displayed or made available to the user.

Wording: The aim is to ensure that consumers understand what the relevant data processing means in practice, and can take a view on what the privacy risks may be for them. Technical expressions or complex types of processing should be explained as far as possible in more simple terms. As highlighted in the ICO's guidance, language should be appropriate to the audience. For example, an app aimed at children should use language a child can understand.

Presentation: The app provider should consider how the information can be most clearly presented, for example displayed on screen as part of the download process, or via a link to a separate privacy notice. The ICO recommends a 'layered' approach, where the most important points are

(Continued on page 6)

(Continued from page 5)

summarised and more detail is easily available if the user wants to see it. Good graphical design, including colours and symbols can also assist with understanding.

Unfortunately, as demonstrated by my Facebook example above, there can also be pitfalls in using concise wording. A short summary, unless carefully drafted, may give an impression of broad-brush and extreme data processing, which is (hopefully) more than is actually taking place. In addition, different devices and appstores may have differing requirements or capabilities for presentation of information. For example, the 'App Permissions' referred to at the beginning of this article are a feature of Android devices, and the choice of presentation and language is to a large extent outside the control of the app provider. An easily-accessible and clear source of further information may assist with clarity and consistency.

'Just-in-time' notifications should also be used, where appropriate. This means that information on a specific type of data processing is provided to the user just before such processing occurs. For example, at the time an app needs to track the user's location, there could be a pop-up notice that GPS data are being accessed. This leads the user to focus on the relevant information, rather than it being hidden in a privacy policy that he never reads.

As noted above, additional consent of the user may be needed for less obvious or more intrusive uses of data. Consent is often required in order to send marketing communications or share data with other parties. It is common for app providers (or the device) to seek the user's agreement to a whole privacy notice or suite of 'permissions' describing all possible uses of data. However, it is preferable for consent to a specific activity to be sought in a separate notice (such as a 'just-in-time' notification) which clearly explains what the consequences are of agreeing to or rejecting the proposed use of data. The provider can then demonstrate that users were well-informed of that particular activity, and a resulting consent is more likely to be legally valid.

Another downside of making a 'catch-all' request for consent is that if a person does not consent, it effectively means that he cannot use the app. As again demonstrated by the survey results referred to above, he may therefore choose not to download the app rather than consent to the whole package of data uses, some of which give rise to privacy concerns. If, instead, more specific consents are sought, consumers who are more privacy-sensitive are more likely to download and use the app in the knowledge they can reject uses of data about which they have concern. This could be achieved, for example, by making the associated app features optional.

As recommended in the ICO's guidance, users should be allowed easily to review and change decisions once the app is installed and in use, such as allowing a user to activate or deactivate features at any time. There should be an obvious place to go to change privacy settings.

Users also have a right to be provided with a copy of any data about them which are being processed in relation to the application. The app provider should therefore provide a clear and easy way for users to make such a request, and provide other feedback, such as a button within the app itself (near the other privacy options), or a specific email address. More detailed guidance on how to contact the provider can be set out within the privacy notice.

If clear contact details and mechanisms such as these are not provided, the app provider may find it has to deal with requests and feedback over less convenient forums chosen by the user, such as Twitter, Facebook or other social media.

The next app instalment

The next two articles in this series will consider the roles of different parties (such as the app developer, the appstore, device operators and data processors) and obligations concerning the security, retention and deletion of a user's data.

Olivia Whitcroft leads PDP's training session, 'Conducting Privacy Impact Assessments'. For further information, see the website www.pdptraining.com

Olivia Whitcroft
OBEP
olivia.whitcroft@obep.co.uk