Apps and privacy Part 2: playing a part

In the second article in a series on software applications, Olivia Whitcroft, OBEP, considers the range of parties involved in creating and managing an app, and their roles in addressing data protection and privacy concerns

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

One app in its time makes many parts. In other words, during an app's lifecycle, there are many different roles for various parties to play. The full production involves design and development, publication and sales, operation and management, provision of platforms, interfaces and related facilities, and storage and analysis of data. There are also other parties who benefit from the app, including users, advertisers and anyone accessing data which the app collects.

Privacy and data protection form part of all of these roles. If you are the app operator, you will need to work with other parties to address the issues appropriately. If you provide platforms for apps, or services for development or management of apps and associated data, you can assist the app operator to address the issues. Whichever part you play, high standards of privacy may be a selling point for your services.

Design and development

Let us start at the beginning. You have an idea for an app, and start to work on design and coding, perhaps with the assistance of a graphic designer or software engineer to bring it to life. Perhaps you undertake some market research, but other than that no live user data are involved. Surely there are no data protection issues to think about at this stage?

In fact, this is the ideal stage to start assessing data protection and privacy matters, so that they are factored into the design and implementation of the app. A review may take the form of a formal Privacy Impact Assessment ('PIA'), or less structured analysis. Everyone involved in creating the app can assist with this, even if they are never going to hold or process any user data.

The security of the app and its infrastructure is an obvious issue (and will be discussed further in the next article in this series). However, security is only one of many considerations.

To take one example, you may want to disclose users' account details to a third party and decide that you will need user consent to do this, in order to comply with data protection requirements. You therefore need to build a way to seek such consent into the design of the application.

To take another example, you may wish to minimise the amount of location data automatically collected by the app, in order to be less privacy-intrusive. Drawing on a scenario raised in the first article in this series (see Volume 14, Issue 3 of *Privacy & Data Protection*, at pages 3-6), you decide that knowing the general vicinity is sufficient, and precise GPS co-ordinates will not be collected. Communications between the app, your systems, the app platform and the relevant devices need to be set up consistently with this.

If you wait until the app is already developed before making these decisions, you may face hurdles in adapting it to meet the requirements, particularly if you have already tailored the app to run on different platforms or link to other applications or websites (see below). It may also delay the launch of the app, and incur additional development costs.

Therefore, designers and developers have a key role in assisting to build data protection and privacy (and not just security) issues into the app from initial conception. Not all designers and developers will automatically take these issues into account, so it will be important to work with them, and to consult with other stakeholders and privacy experts, as required.

Similarly, if you are a software engineer who designs and develops apps for other parties, you can assist your customers by providing options and flexibility in app design to allow privacy matters to be addressed.

Implementation

In order to launch the app, several other parties will be involved (conveniently creating a second 'PIA' acronym):

(Continued on page 4)

(Continued from page 3)

- the providers of platforms ('P') on which the app will run, which may include particular operating systems (such as iOS, Windows or Android), hardware and devices (including mobiles, tablets, PCs, games consoles) and/or other software platforms (such as Facebook);
- providers of other applications or facilities with which the app will interface ('I'), for example if the app incorporates Google Maps, links to a payment provider for in-app purchases, or allows use of IDs from other providers to login; and
- associated app-stores ('A') which publish or sell the app.

As well as coding requirements, clearly the practical capabilities and functions of such platforms and facilities need to be considered.

As the Information Commissioner's Office ('ICO') points out in its 'Privacy in mobile apps guidance for app developers' (copy available at www.pdpjournals.com/docs/88159): 'If you develop for multiple platforms, ensure that you take account of any differences between mobile platforms and their respective appstores — information and features provided by one platform are not necessarily provided by another.'

For example, it would be no good writing an app relying on collecting images for a device which does not have a camera, or relying on a Privacy Notice being displayed in a particular way within an appstore which does not provide this facility.

To the extent that the third party provider is taking actions to address privacy concerns, the app operator cannot simply rely on them without undertaking its own independent assessment as a data controller. For example, Android presents standard 'App Permissions' which may not give a clear picture of the privacy issues. Further steps may need to be taken to clarify.

"To the extent that the third party provider is taking actions to address privacy concerns, the app operator cannot simply rely on them without undertaking its own independent assessment as a data controller. For example, Android presents standard 'App Permissions' which may not give a clear picture of the privacy issues. Further steps may need to be taken to clarify."

Facebook has standard privacy options and controls for users, but anyone building a Facebook app will need to assess whether these are sufficient in the context of that specific app.

Third party providers will also have their own terms, policies and other requirements with which the app provider must comply, and which will impact privacy concerns and how they are addressed. These include terms of APIs (application programming interfaces), SDKs (software development kits), and platform and developer policies. If these are not followed, the providers may prevent the app operator from publishing and running the app (as well as bringing claims for breach of contract).

Common themes include the following:

- requirements to display a clear Privacy Notice outlining how data are used, to keep personal and sensitive data secure, and to comply with data protection and privacy laws;
- restrictions on obtaining information from the platform provider. For example, Microsoft developer terms state that they will not provide developers with access to personal information submitted by customers via the Windows store, and Android developer terms require that if a developer is using an API to retrieve data from Google, they must obtain explicit consent of the user. Facebook places limitations on data which can be accessed if a developer decides to use a Facebook login for an app;
- restrictions on sharing information with the platform provider, other users or third parties. For example, the Google Maps API states that geo-location data which identifies an individual should not be shared with Google without the consent of the user. The Facebook app platform policy states that app operators should not give a user's data to Facebook without consent (although it also allows Facebook to analyse the use of an app, including a user's use of the app) and there are restrictions on sharing data with some third parties even with the consent of the user; and
- restrictions on certain uses of personal data. For example, Google's API terms for advertising and analytics providers state that such parties must not associate an advertising identifier with personal data or a device identifier without consent of the user.

From the other perspective, if you are developing a platform on which applications may run or be published, or allowing others to interface with your app, you should consider how you can promote high standards of privacy and data protection and protect yourself against any damaging actions of app operators. This may include controlling activities of the app operators (through technology, or legal terms and policies such as those referred to above), as well as assisting and assuring app operators and users in addressing privacy concerns.

Hosting and management

It is common for parties other than the app operator to be involved in managing the app and processing data on behalf of the app operator, for example storing, administering or analysing data collected via the app. This may arise because an external party is hosting or managing the application itself, because data servers are hosted externally, or because another party has been specifically appointed to analyse or manage data, or send related communications on behalf of the app provider. Such parties are likely to be 'data processors' and the app provider (as the data controller) will remain responsible for ensuring they handle data appropriately.

Not all third parties appointed to assist in the management of the app or data will need access to users' personal data. If their role is data analysis or maintenance of the app or associated hardware, consider whether information can be anonymised, or whether 'test data' can be provided. The ICO has published an Anonymisation Code of Practice which may provide useful guidance (copy available at www.pdpjournals.com/docs/88160) and the ICO is currently conducting a public survey to review the impact of this.

To the extent that the data being processed can be related back to identifiable individuals, the legal requirements for appointing a data processor must be followed. These include choosing a data processor providing sufficient guarantees on data security, and taking 'reasonable' steps to ensure compliance with those measures.

> ***"To the extent that the data being processed can be related back to identifiable individuals, the legal requirements for appointing a data processor must be followed. These include choosing a data processor providing sufficient guarantees on data security, and taking 'reasonable' steps to ensure compliance with those measures."***

This means undertaking some level of initial due diligence on the provider and carrying out regular checks that measures are being implemented in practice. The app operator must also have a written contract with the processor which requires it to act on the operator's instructions and implement appropriate security measures.

Below are a few tips for app operators to assist in meeting the requirements in practice.

Gain a sufficient understanding of the data flows: What is the processor actually going to do with your data? Is the processor the only party involved in the relevant activities using their own equipment, or are there any sub-processors, for example, responsible for the data servers? Where are servers located and where are data processed? If data are held or processed outside the European Economic Area, there are additional legal requirements to address.

Establish what security guarantees are being provided by the data processor: Ensure that these are understood fully or, if you are relying on the expertise of the provider, you have validated their experience and reputation.

Establish the terms of your contract with the provider: Take particular care if using the provider's standard terms. For example:

- ensure that the third party is not seeking to make any use of the data beyond your requirements, e.g. analysing data for its own purposes. The purposes for which data may be used should be restricted within the contract;
- consider what specific security guarantees are being offered. Contracts often contain the basic clause to implement appropriate technical and organisational security measures, but are you clear what this means in practice? Ideally, the contract should provide greater clarity on specific security measures and controls. This topic will be discussed further in the next article in this series;
- consider what ongoing practical control and guarantees you will have, for example can you require an audit or request confirmation of compliance with the contract and security standards;
- make sure that the provider is obliged to delete or return data at the end of the contract, or at any stage upon your request; and
- treat privacy and security as material obligations. For example, do you have a right to terminate the contract and seek compensation (for yourself and affected individuals) should the obligations be breached?

On the other hand, if you are a data processor, you should consider how you can assist app operators with compliance and privacy, and assure them that you are doing so. As raised above, this could be a selling point for your services. If you can demonstrate appropriate expertise in security and privacy as well as, or as part of, the core services you are offering, app operators can be confident that they are meeting their obligations as a data controller. If you do wish to make your own use of any data beyond that required by the app operator, be aware that you will need to work with the app operator to ensure lawfulness and transparency, including obtaining appropriate consents from the users.

Users

Users of the application need to be involved with their own privacy and

(Continued on page 6)

(Continued from page 5)

the privacy of other users. This includes providing users with clear information and giving them appropriate options to control the extent to which data are collected, used and shared.

Since the writing of the previous article, the UK's Office of Fair Trading has published principles for app-based games, which app providers must follow in addition to data protection requirements. These require consumers to be provided with sufficient information about how their data are collected and used, what payments may be required, and with whom data may be shared. A copy of the principles is available at: www.pdpjournals.com/docs/88161

As well as the issues with sharing data with other organisations (discussed below), app providers need to consider the extent to which user data are shared with other users. For example, is a user permitted to search for friends using the app? Does the app use location technology which allows a user to see the whereabouts of other users? Will the user's score in a game or quiz be displayed to other users? As well as ensuring such activities are 'fair' and not excessive, they need to be factored into privacy notifications and options. As noted above, the app operator will need to work within the boundaries of the platform provider's requirements. For example, Facebook requires that operators allow users to control which activities are posted on their timeline for 'friends' to see.

In addition, the app operator should consider whether it can address risks of a user misusing other users' data within its app policies and terms of use, with which users must comply. This may include limitations on how the app may be used, and obligations in relation to use of information. The app could include facilities to detect and report misuse. Such terms must be clearly presented to users (in the same way as Privacy Notices), and there must be actual consequences of failing to comply, which may include accounts being de-activated or other legal action.

Sharing data with other parties

The app operator may wish (or have agreed) to share data collected via the app with other parties. Data can be a huge asset, providing information on social trends, preferences and behaviours, including activities undertaken and places visited. The app operator may wish to publish information in order to promote the benefits of the app, or provide it to specific third parties in return for money or other consideration, for example promotion or improvement of the app, or enabling its compatibility or use on specific platforms or within specific locations.

As raised above, a key consideration is whether data identifying individuals needs to be shared, or whether providing anonymised information can achieve the same goal. This will depend on whether the purpose behind the sharing relies on knowing details of specific individuals, for example to send direct marketing materials, or whether anonymised trends and statistics are sufficient, e.g. for general analysis of app usage. True anonymisation is not always easy to achieve. Consideration needs to be given to whether, in the hands of people with specific knowledge, the information can be traced back to identifiable individuals. As noted above, the ICO's Anonymisation Code of Practice may provide useful guidance.

If the intention is to share personal data which identifies individuals, it is generally difficult to justify this without the consent of the user. The method by which consent is obtained needs to be appropriate to the nature of the data and the purposes of the data sharing. Explicit consent will be preferable; however, where the data sharing is inherent to the objectives of the app (for example if the purpose of the app is to facilitate a transaction between the user and another party), an implied consent or other legal justification may be sufficient.

There is also the question of whether a party with whom data are shared is an independent data controller or a joint data controller with the app operator. This will impact where ultimate legal responsibility lies.

If the app operator is collecting certain data for the sole purpose of sharing it with a third party, it could even be the case that the app operator is a data processor on behalf of the third party data controller (for those particular data). Assessing precisely who is a data controller and/or data processor, and to what extent, can be very difficult. Without drilling into the detail, it may be more practical for the parties to work together to ensure that data protection requirements are met. The app operator should be careful not to agree contractually to share data with another party without further consideration of where the responsibilities lie for data protection compliance, and how these will be addressed. It would be prudent for the contract to allow the app operator not to share information to the extent data protection requirements are not met. The app operator could find itself in breach of data protection laws by sharing data inappropriately, as a contractual obligation to share data is not a legal justification under data protection laws.

Casting the roles

There are many parts to play in developing and operating a software application. Privacy considerations should form part of the casting process for those roles. In some areas there may be limited choice. For example, in order to obtain the widest user-base, a mobile app may need to run on iOS and/or Android platforms. The app operator may have limited power to negotiate requirements and must work within the boundaries set by the providers of those platforms. There will be a wider choice of parties to assist in developing the app and managing the data, or with whom data are to be shared. The matters highlighted in this article will influence such choices and the terms on which relationships are formed. Getting the roles right will enhance compliance, public image and reputation, ensuring privacy and data protection are built into each performance.

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