Apps and privacy Part 3: appropriate security and retention

In the third and final article in this series on software applications, Olivia Whitcroft, principal of OBEP, considers how to keep apps and their data secure, and reminds app providers that user data should not be retained indefinitely

The media is regularly packed full of stories on information security flaws and breaches, putting individuals' data at risk. We all know that 'appropriate technical and organisational measures' must be taken to protect personal data, but how do we achieve this for software applications?

By their nature, the use of apps presents security risks. Apps allow the collection, storage and communication of data on the move, using a variety of software, devices, systems and networks. The app operator will need to assess how it can secure the app and its own databases without (necessarily) having control over the security of the device, its operating system, the communications network and other third party systems involved.

When it comes to data retention, personal data should not be kept for longer than is 'necessary' for the purposes they were collected, and should be securely deleted. In the context of apps, it is unlikely that app operators will delete all data about a user the moment that user stops using the app. However, further retention and use needs to have a legitimate justification and, at some stage, even that justification will expire.

This article discusses information security measures which should be considered in relation to apps and — to complete the lifecycle of the app and its data — the retention and deletion of user data.

Information security — what standards must be met?

Data protection law requires that 'appropriate technical and organisational measures' are taken against 'unauthorised or unlawful processing' of personal data and against 'accidental loss or destruction of, or damage to' personal data.

Data protection laws are, of course, not the only reason to keep apps and associated systems and data secure, nor do they describe the only standard for information security. Indeed, the standard they set, as quoted above, is open to interpretation in context. Compliance is not a 'tick-box' exercise; it requires an assessment of risk and adoption of measures to reduce those risks. Knowledge of information security as a separate specialism is therefore needed in order to meet the data protection rules in practice.

This is particularly important in rapidly developing areas of technology, such as mobile applications. In assessing security, we need to look beyond catchphrases such as 'password protected' or 'encrypted', and consider the detail of how apps, devices, and servers are accessed, how they communicate with each other, and how and where user data and passwords are stored, retrieved and used. System and data flow diagrams, which highlight security touch points, may assist with visualising and understanding this in practice.

Authentication and passwords

Usernames and passwords may be used to authenticate a user in order to access an app (or part of an app's functions). This assists in preventing unauthorised access to the app, the app's services and/or the associated data. It then becomes necessary, of course, to ensure the usernames and passwords themselves are kept secure from unauthorised access or use.

Security flaws in apps may arise from the methods of authentication of users and how and where passwords are stored. In January 2014, there were reports of a Starbucks mobile app (in the US) storing usernames and passwords used for purchasing coffees in plain text within a user's device. This was apparently to recognise the user so they did not have to log in each time they accessed the payment function. However, it meant that if the device was compromised, a third party could easily extract and re-use the username and password on another device. Further, if the user had the same username or password

(Continued on page 4)

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

(Continued from page 3)

for other apps or services, these are now also at risk.

As an alternative mechanism to recognise a user, an app operator could issue the device with a separate authenticator (which is not the password itself, but requires the password when issuing it). This may also be vulnerable to attack, although potentially could be tied to the device to limit the extent of potential misuse.

Encryption of passwords is an option, but may be of limited benefit to protect a single password, as another password is required to decrypt it!

Where an app duplicates services which are also accessible by other means (for example via a web browser), the app could have more limited functionality (for example not allowing substantial account alterations) in order to minimise misuse should the device or its authenticator become compromised.

"Where an app duplicates services which are also accessible by other means (for example via a web browser), the app could have more limited functionality (for example not allowing substantial account alterations) in order to minimise misuse should the device or its authenticator become compromised."

Security must also be considered in the mechanism for validating a password entered into the user's device and received by the app operator's systems. It is common for a password to be hashed and salted by the app operator, and this is also recommended within guidance from the UK data protection regulator (the Information Commissioner's Office) on privacy in mobile applications. Essentially, this converts the password into an unrecognisable string of text, which cannot be reversed or decrypted.

The app operator stores only the hashed and salted password, and not the original password. This means that if its password database is compromised, the hacker does not know the actual passwords used by individual users.

Communication of data between the app and data servers

Communication channels between the user's device and the app's servers are commonly encrypted to protect data in transit, rather than relying on the security of the telephone or Wi-Fi network. The databases on which data are stored or the data itself may also be encrypted for storage or transit.

The ICO's guidance recommends that app developers should not re-invent the wheel with encryption. It states: 'Use tried and tested cryptographic methods, rather than implementing your own cryptography. Whether the purpose is for transmission or storage, research the most appropriate cryptographic methods and use established implementations of them.'

However, the app operator must also stay on top of any particular vulnerabilities or requirements for implementing standard cryptographic techniques appropriately. The ICO raises particular recommendations in checking TLS/SSL certificates and ensuring they are configured correctly on a central server.

In addition to encryption of the communication to the data servers, the app operator must consider any vulnerabilities in the software used to enable information being created by the app to be interpreted by the app operator's servers, i.e. the application programming interface (API) between the two. On New Year's Eve 2013, hackers published 4.5 million usernames and (partially redacted) phone numbers for users of Snapchat, a photo messaging application. Hackers had reportedly exploited flaws in Snapchat's API used to match mobile numbers to Snapchat usernames as part of a 'friend finding' facility, in order to gain access to this data.

Data stored on user's device

Not all user data are stored on (or only on) the app operator's servers, and (as well as passwords described above), some user data may be stored locally on the user's device. This may be on the device's hard drive, the SIM or SD card.

As well as the user (and anyone who has the device) gaining access to such information, third party applications may be given access to the SD card or other storage facilities on the device. Although this is hopefully with the user's knowledge and potentially consent, for example using 'App Permissions' (see the first article in this series, pages 3 — 6 of Volume 14, Issue 3 of *Privacy & Data Protection*) the app operator must assess what additional vulnerabilities this presents. The impact may not be entirely clear to users, even if they have granted permission.

In early March 2014, there were claims that WhatsApp, an instant messaging app, was exposing chat content by saving it on the SD card of a user's Android device. The content may be unencrypted or encrypted depending on the app version. These could be accessed by any other Android app which was given access to the SD card. WhatsApp reportedly claims the risk is overstated, and that the data are only vulnerable to malicious apps or viruses. Nevertheless, it highlights that the more data that are stored on a device, the

more vulnerable such data are to misuse. Further, some of the risk may be down to Android or other operating systems' approaches in granting access to device or SD card content.

Interface between the app and third party apps or systems

As discussed in the second article in this series (see pages 3 — 6 of Volume 14, Issue 4 of *Privacy & Data Protection*), it is common for apps to collect or share information from or with third party apps or facilities, for example in order to retrieve a user's location, photos or contacts (using other facilities or apps on the user's device), to authenticate a user with credentials from a third party app (such as Facebook or Google) or to share user data with a third party controller or processor (for a legitimate purpose).

The app operator should assess the security of the communication method (in the same way as communication with its own systems as described above), and check there are no vulnerabilities in accepting data from the third party. The ICO's guidance raises the risk of inter-app injection flaws. Data received from the third party could (either accidentally or deliberately) cause the app to perform unintended actions, or contain a virus or other malicious content.

The app operator should also consider the overall reliability of third party data and systems, and any potential exposure from third party security flaws. For example, if the app uses a third party login, and that party suffers a security breach, it may also expose access to the app users' accounts.

"The app operator should assess the security of the communication method (in the same way as communication with its own systems as described above), and check there are no vulnerabilities in accepting data from the third party. The ICO's guidance raises the risk of inter-app injection flaws. Data received from the third party could (either accidentally or deliberately) cause the app to perform unintended actions, or contain a virus or other malicious content."

To what lengths do you need to go?

Data protection laws do not require the highest level of security for all aspects of every application and system. Security measures must be 'appropriate' to the nature of the data and the harm that may result. They may also take into account the cost of implementing the measures.

So, for example, an app which collects and uses financial information or sensitive personal data may require higher security standards than an app providing information on local places to visit. The app may have different levels of security for different functions. For example, when the user moves to a payment area, this may require further authentication than to access the other areas of the app.

Nevertheless, it is difficult to imagine an app which does not present any level of risk. Therefore, some consideration of security in the areas described above will generally be required.

The ICO suggests undertaking vulnerability scanning or more in-depth penetration testing to identify potential problems.

Data protection rules also require he 'state of technological development' to be taken into account in deciding on appropriate security measures. As the ICO points out, the app operator should regularly check that security mechanisms are still up to date and relevant, especially as operating systems introduce new features and state of the art progresses. To put it another way, app operators should keep themselves *app-rised* of app developments.

Other technical and organisational measures

App operators must not forget other practical security measures applicable to its systems and procedures. This may include (amongst others) physical security of its offices and data centres, training of staff, governance and responsibilities, policies and procedures, and access rights and controls for its premises and systems.

Link between security and other data protection principles

Decisions on security measures should be made in consideration of the other principles of data protection, such as fair processing of personal data, limiting use to defined purposes, and ensuring excessive data are not collected. Security features will assist in ensuring, for example, that use and sharing of data is not 'unfair', that the app does not collect more data than it needs, and that staff of the app operator do not have access to data beyond that required for stated purposes.

Security measures are also one of the considerations in assessing whether there is 'adequate' protection for any transfers of data outside the EEA.

(Continued on page 6)

(Continued from page 5)

Retention and deletion of data

As has been described in this series of articles, the operation of an app may involve the collection, use and storage of substantial amounts of user data. The app operator needs to identify how long user data will be retained, and ensure that the data are securely deleted or potentially returned to the user when no longer needed. Of course, the longer user data are retained in any location, the longer they are vulnerable to security breaches; an additional benefit of deleting unnecessary data.

Data protection law requires that personal data are not retained longer than is necessary for the purposes for which they were collected. The primary purpose of collecting user data is likely to be to provide the app's services. Data will no longer be needed for that primary purpose once the service has been provided. This may be because the individual stops using the app, or because individual transactions or services using the app have been completed, or because the app operator decides to stop providing the app or its services.

The app operator then needs to consider how long after completion of a service or transaction it needs to retain data for legitimate legal or commercial purposes. Such reasons should be documented and retention periods set, which may be different for account data, transactional data and other content. Retention and deletion should take into account all different locations where data may be stored, including on any systems of data processors. The app operator may need a mechanism to identify that an app is no longer in use, for example through regular checks for inactive accounts or logging when an app has been uninstalled.

Data must of course be deleted in a secure manner, using appropriate technical expertise to ensure those data cannot be retrieved. It may be useful to highlight if the user him/herself needs to take any further steps to delete data (such as from his or her own device).

The app operator should also consider how long data will continue to be made available to users, and in what format, such as details of past transactions, messages, photos or other content. This may be a facility to assist users in retrieving information which they may want to keep, or a procedure to respond to subject access requests for data which the operator is retaining for its own purposes. Taking into account security concerns, it may be appropriate to provide longer-term access using a mechanism separate to the app itself, for example over a secure web interface or upon separate request to the app operator.

As outlined in the first article in this series, if the app operator wishes to continue to make use of user data for wider purposes unconnected with the app's services (such as analysis, marketing, profiling or data sharing), these must be clearly explained and brought to the attention of the user, preferably at the time the data are collected. The consent of the user may be required. It may also be useful to remind users of the extent to which data may be retained for ongoing purposes (or deleted), rather than just relying on notifications given upon collection.

The proposed new EU Data Protection Regulation, which may come into force within a couple of years, should also be borne in mind when creating retention procedures. The proposed Regulation includes (within early drafts, at least) the hotly debated 'right of portability' and 'right to be forgotten'. If adopted, these would enhance existing subject access rights and requirements not to hold data longer than necessary. They could require user data to be packaged up and returned to the user, and wiped from all the app operator's systems.

App-end-ix

We have reached the end of the lifecycle of the app and this series of articles on apps and privacy. We have looked at the extent of data an app collects, ensuring users understand how their data are being used, the roles of different parties involved, keeping the app and its data secure, and, finally, deleting user data securely when those data are no longer needed. App operators and others involved in creating and managing apps and their data can develop their *app-roach* to building data protection, privacy and security into the architecture of their app.

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