Project Specification LSEPI Analysis – Android Attendance Monitoring

Module Code 55-403325

Introduction

The purpose of this report is to analyse the details of a computing project brief and both identify and discuss some legal, social, ethical and professional (LSEPI) issues which may be apparent in the project brief while referencing real-world examples of effects and consequences of these issues.

Herein "Legal, Social, Ethical and Professional" may be abbreviated to "LSEPI" and the project brief specified below may be referred to as "the specification" or "the brief"; the project outlined by the brief "the project".

The Project Brief

The project brief selected for this report is the 6th example provided, which proposes the use of an Android application developed for the project to track attendance of events, jobs or reoccurring classes or lectures.

The full title of the project is "An Android mobile application to record and monitor attendance with a look into modern technologies."

Main Issues

Issue – Processing and Storage of (Minors') Personal Information

One of the main issues with the project specification is the fact that since it is not a bespoke product being designed but rather a system that can be applied in many different circumstances, it is always a possibility that minors could come into contact with the system and become users of it. Since the app is used to track individuals, there must be some kind of identifying property to their login or installation of the app, which would likely be their full name and some basic information like date of birth, and maybe a photograph – this is all classed as personal information under the General Data Protection Regulations.

Thus, the appropriate laws must be accounted for in the design and privacy of the app and the way that consent is gained from the user to access certain permissions on their device.

It is important to note that while this app would merely be scanning a QR code or even taking a manual log of attendance (or potentially scanning an NFC chip), this information could be used to determine the whereabouts of the user based on the registered location of the logged attendance.

Issue – Lack of Multi-Platform Support

It is stated in the specification that there are plans to develop an Android app for the system, but no other platforms are mentioned besides the possibility of Android-based wearable devices.

This instantly places a massive restriction on the uses of the system, as it means that only certain people (those with devices running Android) would be able to use the app. While it could be argued that the app is only in initial stages, this would almost certainly limit the system to being used in

specific cases for testing only until an app for other platforms (at least iOS) can be developed and released for people to use.

Issue – Possible Security Flaws

In the Project Aims section, it becomes apparent that the person developing the specification does not currently know how to develop Android apps.

This presents a major issue, as if the project planner is this new to app development, it seems likely that there will be flaws in the app due to their inexperience that could compromise its security – not good news when there are strict data protection regulations to follow especially since the system will likely be used by minors.

Impacts and Examples

Processing and Storage of (Minors') Personal Information – Impacts

Looking back at the addressed issue of the potential processing and storage of minors' data on the app/system, we can reference current General Data Protection Regulation (GDPR) rules surrounding the matter to see what kind of measures must be taken to comply:

"…The processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child."

(GDPR Info, 2018)

There are multiple ways that this issue could be approached, and each would have different impacts on both the development process of the application and the final result.

The first, and possibly most obvious, is to just make sure that all parts of the app and system are secure and comply with the GDPR rules – this would include measures such as:

- A consent form when signing up for the app which explicitly mentions that children under a certain age (dependent on country) must have parental consent
- The servers on which user data for the app are stored on (if there are any) must be secure and well-maintained, with well trained staff interacting with the system, to minimise the risk of a data breach involving the personal data of registered users.

Another method would be to eliminate the possibility of those under the age of 16 using the app – it would be possible to include in the end user license agreement for the system that no persons under the age of 16 are permitted to use the app, and this would perhaps line up with a feeling that children of that age should not be responsible for tracking their own attendance anyway.

However, this would be a restrictive approach as there may be other similar products which do allow under 16s, and many of the same GDPR rules would have to be followed regardless due to the processing and storage of personal information; tackling the issue of parental consent for minors on top of this would not be a lot of hassle.

Lack of Multi-Platform Support – Impact

The lack of a version of the app available on one of the two major mobile operating systems is an extremely limiting factor, so much so that unless a company exclusively provided its employees with Android devices and no other mobiles were allowed on-site, it is difficult to imagine the system being purchased.

The impact here is clear – if the app developed for Android functions well and is ready as a product, it could possibly be deployed in a few places whilst an iOS app (and others) is developed. Otherwise the app would need to be developed for at least both Android and iOS platforms before being marketed to the public.

Possible Security Flaws – Impact

The prospect of an inexperienced app developer going straight into deploying an app handling processing and storage of personal data seems quite daunting – surely the app would have countless bugs and flaws which could facilitate security breaches?

Well, yes, but as with any app like this, rigorous testing and examination and maintenance of app code would ideally give the same result as any experienced app developer, in terms of security.

It would be a good idea to have a 3rd party inspect the application's code and test the front-end user experience for bugs and flaws, to try and remove the chance of any breach of data due to poor app or code design.

The possible impact of a data breach due to security flaws in the app could be immense – under GDPR, fines can be up to €20,000,000 or 4% of the company's total turnover from the previous financial year (GDPR Info, 2018).

An example of a fine under the new GDPR rules is when British Airways suffered a large data breach and faced a £183 million fine over the incident (Cellan-Jones, R. 2018). Considering the small scale of this project, the fines would obviously be nowhere near this big but could still be a big hit to the business.

References

Cellan-Jones, R. (2018). *British Airways faces record £183m fine for data breach.* BBC Business. Retrieved November 11, 2019

GDPR Info. (2018). *Art. 8 GDPR*. Retrieved November 11, 2019, from gdpr-info.eu: https://gdpr-info.eu/art-8-gdpr/

GDPR Info. (2018). *GDPR Fines / Penalties*. Retrieved November 11, 2019, from gdpr-info.eu: https://gdpr-info.eu/issues/fines-penalties/