ASSESSMENT 1 — Case Study Analysis

1. Human Factors issues in this case

a) Frequent pop-up trip reminders may overwhelm the user, making the system difficult to use. The reminders are intended to be a notification for emergency situations, including late for the user's flight and wrong gate. If the user could manage the trip details and get to the right location on time, the reminder should be muted for a better experience. It has been claimed that lots of notifications could reduce the user's concentration.*(Benyon, D. 2019, p. #)*

b) The user should log into the system everyday. This issue may burden the user, as it feels similar to an unnecessary alarm clock reminding you to go to work every day, but for a system you wouldn't use everyday. For many people, it's difficult to form a habit of doing something that isn't important. And this requirement could pose significant challenges to maintaining user loyalty, which has claimed by *Richard L. Oliver (1999, pp.33–44.)*

c) Using two-factor authentication for each log in in the new system is also a burden to user because sometimes the two-factor authentication could be very complicated. This authentication would send a one-time code to the user's mobile phone. When the user comes to a place with poor signal, they couldn't get the code and log in.

d) Migrate all the users on the mobile system is also a human factor issue. Since we had all our users on the web system and we want them all would use the new mobile system, the action we could take is migrating the users. But to the users they might not know that the system is replaced and they wouldn't be able to find the new mobile system by the instructions we provide. Also, the users would spend time to learn how to use the new system and get used to it.

2. Ethical issues in this case

a) Tracking the user's trip data without permission is a very important ethical issue in this case. As we mentioned that the web system could send pop-up reminders to notify the user for the trip's agenda, but we didn't mention that how would the system know the user's trip. Is reading the data be allowed by the user or not? If not, it would be a huge infringement of user privacy and the users wouldn't know what would happen to them by reading their trip data, and some unfortunate things had happened because of that. It has been claimed that invading user's privacy could be both personal and environmental problems. *(Floridi, L. 2013, p. #)*

b) The ads may cause infringement of user privacy too. As we all know, the advertisements could bring us a lot of revenue, but it may hurt the users by pushing them a lot of inappropriate contents, and some could be really offensive. This action should be permitted to access by the user, otherwise we are breaching the rules of privacy and consent principles. The user could sue us for this.

c) Deleting the user data in 366 days since the last log in without permission is another ethical issue. The user should know our policies of data keeping and deleting. If we want to delete the data, we should let the user to do it but not we force it to be deleted, which is a reflection to the respect to the principles of autonomy. Also it has been claimed that users should keep their rights once they need to delete their own data *(Nissenbaum, H. 2009, p. #)*

d) Keep the user's phone number without permission is also an ethical issue of users' privacy. The user's phone number is just for registration and two-factors authentication, but we should ask the user for permission to send code to their mobile device. And we must promise that we wouldn't use their phone numbers for any other purpose, including but not limited to selling the phone numbers for extra profit, sending them promotion text messages and so on. Once we get the user's fully permission we should only use the phone number as we promised.

3. Improvement with the issues above

First we should solve some ethical issues problems, as we mentioned we were lack of lots user's permission. We should pop our user privacy policy and data privacy policy after the user's very first log in. If the user chooses to not give the permission the system would automatically shut down. Next we should cut the user data automatically deletion after 366 days since the last log in. We should make sure that all the decisions should be made by the user self not us. Then about the advertising part my suggestion is we should offer the user a choice to close the advertisements because not all of the users would be happy to see the advertisements. The last but not least is that make a promise before asking users to provide their phone numbers and never break the promise.

Then we could focus on the human factors. There's no need to make user log in once a year so after we get the permissions to save the user data, we should keep it and not force the users log in. And the same to the two-factor authentications, which should be less frequently than every log in, but still for the security, only makes it one time for three months. We should also cut the pop-up reminders and make it a configure setting page for users to choose their own frequencies, such as only before trip, everyday or never. Of course it would only notify after we get the permission to read the user's data.

Reference list

Benyon, D. 2019 *Designing user experience : a guide to HCI, UX and interaction design*. 4th ed. Harlow, United Kingdom: Pearson Education Limited.

Floridi, L. 2013 *The ethics of information*. Oxford Oxford University Press Oxford Oxford University Press.

Helen Fay Nissenbaum 2009 *Privacy in context : technology, policy, and the integrity of social life*. Stanford, Ca: Stanford University Press.

Oliver, R.L. 1999 Whence Consumer Loyalty? *Journal of Marketing*, [online] 63(4), pp.33–44. Available at: https://foster.uw.edu/wp-content/uploads/2016/07/12_Oliver_1999.pdf.