COMP3020 COURSEWORK 2

– CASE STUDY ANALYSIS

Student Name: Chaeryeong Kim

Student ID: 20206447

Date of Submission: 20.12.2019

Word Count: 1887

Declaration: *I confirm that this coursework submission is all my own work, except where explicitly indicated within the text.*

1. Project Title and Description

The project I have chosen to discuss in this case study is the Developing a Dating Application which I belonged to the software development team of for my sophomore year project. The aim of the project was to create an android application of matching services for users. The idea behind this project is to provide a safe platform for users who prefer to start a new relationship through an online service.

When joining the application for the first time, users are required to submit their personal information, I.e. name, age, university, 3 photos, job, company, town they reside in, and personal preferences. If they don't want to be matched with their acquaintances, the access to the address book should be allowed by users additionally. Based on these data, users are recommended every day up to 10 people who are likely to prefer and can send messages using virtual currency to those they want to meet and date with. At this time, recommended people can access each other's profiles for 24 hours, right before a new recommendation.

The development team was composed of 3 developers including me and a guidance professor supervised the whole process of development so that the application can be released on the market in a few years.

2. Ethical Issues

2.1. Privacy and Personal Information

Personal information is data that relates to a living individual who can be identified from that data either on its own or combining with other information (Jay, R.). Due to the characteristic of the dating application, which is to suggest recommended candidates to users based on personal information provided by the users and other users, the system database of the application of the project stores a vast quantity of users' personal data including name, age, university, photos, job, company, town they reside in, personal preferences such as sexual orientation, preferred dating activity, etc. and also the result of the matchings. These listed data are regarded as personal information protected by the law of EU General Data Protection Regulation (GDPR) and UK Human Rights Act 1998 which means that collecting and disclosing personal information without the users' consent violates the law. Breaching the law, also expressed as being illegal, is considered as immoral in the society in the law. If this information is leaked to others without consent and notification in the process of matching, it's definitely disobeying the law. Therefore, software developers should design and develop the code and proposed algorithms to prevent this morally unacceptable situation from happening since they are morally responsible to conform to the law.

A similar and related issue about privacy in this year is the leakage and misuse of the user's personal information of the Korean dating mobile application called 아만다 (I.e. Korean word meaning do not date with anyone.) (WIKITREE, 2019). 아만다 is an online dating matching service company providing a mobile application for the service and it's one of the most widely used dating application in South Korea. 아만다 collects the users' information including name, age, photos, job, residence, and body profiles such as height and weight to match users using the collected data. However, due to the blind spot of the software code, the account of the administrator rights, called "Super account", was leaked so that the ordinary users could access the data of other users in the application. The company explained that it fired the related software developer and strengthened its privacy

system so that this kind of disaster would never happen again. The consequence of this data leakage and disclosure is quite server in the point that loads of users became to go through a situation that they didn't want which is considered as a breach of privacy and it's more serious in the context that a privacy right violation is a violation of another right (Judith J. Thomson, 1975).

If the application of the project is unable to ensure the users' personal information securely as the case mentioned before, the software developers are considered immoral because they overlooked or paid less attention to implement an adequate application even though they know or should have known the serious consequences of the violation of the privacy and the importance of protecting it before it happens. Plus, they are also ethically responsible referring to the Rule Utilitarianism since they caused damage to users as they disobeyed the rules "do not cause pain", "do not deceive", "keep your promise", "obey the law", and "do your duty". As long as the project aimed to provide a safe platform for online matching, it is software developers' promise and duty to ensure safety regarding protection of personal information which is securing users' privacy. This discharge of duty can also be supported by ACM Code of Ethics 1.7 which says to respect the privacy of others and it's the responsibility of professionals to maintain the privacy and integrity of data describing individuals (ACM Council, 1992). Therefore, the software developers are morally and ethically responsible for ensuring the safety of personal information in the process of developing and implementing the application in the view of privacy.

2.2. Reliability of Avoid Matching to Acquaintances

One of the main functionalities of the dating application in the project is to avoid being matched with users' acquaintances. Once recommended and matched, the list of photos and profile of candidates are visible to each other which means the user can notice that he or she is matched with his/her families, friends, or colleagues right away and the fact that the counterpart is using a dating application which user may want to hide. The acquaintance-avoiding function is able from accessing the users' address book in the mobile after his/her consent thus, it might not work correctly if the people modify their phone numbers or do

not keep others' phone number even though they know each other. In this case, the application cannot ensure the dependability and especially fail to provide reliability which is the continuity of correct service. The dependability of a computing system is the ability to deliver service that can be justifiably be trusted according to the 8th lecture material. When the application cannot provide a dependable software in the context of avoiding functionality, the users will suffer damage that does not benefit from the function even though the relevant information is provided. Then by the rule "keep your promise" of rule utilitarianism, the software developers are asked for ethical responsibility for the failure of the reliability. Here, we can also ask them for the moral responsibility according to the 3 criteria listed below suggested by D.Birsch (Birsch, D. 2004).

1. The action of the person must have caused the harm or have been a significant causal factor.

2. The person must have intended or willed the harm, or it must be a result of his or her negligence, carelessness or recklessness.

3. The person must have been able to have known, or must know the consequences of the action, or must have deliberately remained ignorant of them.

Regarding the first criterion, it's obvious that user suffers from the harm caused by failure of reliability of the function because they are unexpectedly disclosed that hey are using the dating application to the colleagues/families/intimates and might be ashamed that they ran into the boss online.

Although the developers didn't break the reliability of the application on purpose, they cannot avoid the second criterion since it's their profession and duty to implement the key function to keep the correctness in the use of the application. According to the rule 1 of IT Ethics of Keith W. Miller, the people who design, develop, or deploy a computing artifact are morally responsible for that artifact, and for the foreseeable effects of that artifact. This responsibility is shared with other people who design and develop (Keith W. Miller, 2011).

Also, the third criterion justifies that software developers are morally responsible since at least they must know the impact of the action as long as they know the importance of the functionality.

To sum up, the software developers of the project are both ethically and morally responsible for betraying the reliability of the acquaintance-avoiding function which is promised to avoid matching with users' associates.

3. Proposed Way Forward

3.1. Protecting Users' Privacy

To protect the privacy of the users with certainty, first of all, the application should explicitly and repeatedly show a "Terms and Condition" with all privacy policies of the application for users. It must include every single point of information the application may collect and store. It should also clearly state when the information is stored and deleted in the system database of the application. The personal information of the user should be collected and stored from the point the user explicitly agreed by pushing the agree buttons for every condition and deleted when the user withdraw the agreement or the user unsubscribe the application. This means that the user can always agree and disagree when he or she wants to.

The application also should clearly state that the agreed and collected information is used only for the proper purpose which is making a recommendation to suggest several candidates to users. In addition, the application should specify to users what information among the data they provided the counterpart user can access to so that the users can respect others privacy as well too and be notified that only part of their information would be accessible from matched users.

To reassure users that the incident like the above-mentioned case are not going to be happen in the application of this project, the application shall expressly promise not to use or leak the administrator account outside of its administrative purposes and declare its conscience. For just in case, privacy risks and loss that would be brought when it comes to the crunch should also be listed so that the users can be aware of the damage of a contingency according to the opinion that the privacy risks and loss should not be invisible (L.Jean Camp, 2015).

3.2. Avoid Matching to Acquaintances

To successfully maintain reliability of the key functionality of the project which is to avoid being recommended and matched with the people the user knows when the user required the function and agreed on access to his/her address book in the mobile, several approaches can be adopted to the application and development team. The first method is to use more information user provided such as university and company or even job. This would make wider avoidance possible because by using more data than the address book the software developers are able to implement the function to operate with filter codes on wider categories. Here, the software developers should not forget to request additional agreement and notify users for the application to these data for this functionality. The second approach is applicable to development teams which is to clarify the issue and develop alternative ways of thinking about the improvement in the context of artificial agents. For this, the application project team shall work more actively with professors, engineers, and software validation specialists from different fields of computer. Different specialists will likely take different approaches on implementing (Colin Allen, Wendell Wallach, Iva Smit, 2006). Lastly but not least, the software development team should spend more effort for validation of the function.

References

ACM Council, ACM Code of Ethics and Professional Conduct, Retrieved from ACM: http://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct#CONTENTS, Accessed 19 December, 2019.

Guide to the General Data Protection Regulation, Jay, R., & Jay, R.

Moral Responsibility for Computer Artifacts: The Rules. Keith W. Miller, IT Professional, Vol. 13, No. 3, pp. 57- 59, IEE Press, 2011.

Moral Responsibility for harm caused by computer system failures, Douglas Birsch, Ethics and Information Technology 6 (4):233-245 (2004).

Respecting People and Respecting Privacy, L.Jean Camp, Communications of the ACM, Vol.58, No.7, pp.27-28, July 2015.

The Right to Privacy. Philosophy & Public Affairs, Thomson J., *4*(4), 295-314 (1975)

Retrieved from www.jstor.org/stable/2265075

Why Machine Ethics?, Colin Allen, Wendell Wallach, Iva Smit. IEEE Intelligent System, pp. 12- 17, July/August 2006.

WIKITREE, 소개팅 앱 '아만다' 임원, 회원 정보 '무단으로' 열람해 보고 있었다, 2019,

Retrieve from WIKITREE NEWS: https://www.wikitree.co.kr/main/news view.php?id=470782, Accessed 18 December, 2019.