Sion Gregoire IRADUKUNDA
29001816

Project specification LSEPI Analysis

A prototype mobile application to track users' daily activity and symptom pain to aid self-help

This project aims at improving people's standards of living by tracking their daily routines using activity/fitness tracking technology. The main data recorded relates to diet, exercise and sleep. The application will then give suggestions on how to improve the user's health condition based on the data collected by helping them better understand the relationship between their diet, sleep, exercise and their symptoms or health condition. For convenience, the application will mainly run in the background or at scheduled times and notify the user when to enter their daily experience of pain and any other useful information. The application intends to be as non-intrusive as possible and will also not require manual data input from the user at all times.

One legal issue or concern with this application is related to the collection of the users' data. The data gathered by the application include private or personal information about the user and if leaked to unauthorized parties, it could lead to many negative outcomes on both the user and the company (application developer).

If the data is leaked, the company will be breaking the law especially the 2018 General Data Protection Regulation (Information Commissioner's Office, 2018) and many other data protection legislations including but not limited to Data Protection Act 1998 (legislation.gov.uk, 1998) and Data Protection Act 1984 (legislation.gov.uk, 1984). If the company breaks the law, it will eventually get fined and this will heavily affect its finance and reputation even if the leaks might have been accidental. An example of this is the recent fine on British Airways of £183 million due to passenger data breach (Sweney, 2019).

On the side of the user, the personal data collected, such as the user's sleep schedule and what time they exercise—if leaked to thieves— could lead to a well-planned burglary. This data if accessed by the thieves, would give them an advantage as they would know exactly when the user is at their most vulnerable state; when sleeping or is not at home. This would result in a case similar to the Marriott data breach in 2018 (Chapman, Anderson, & Bajak, 2018) which has the potential of leading to home burglaries, espionage and ID theft.

Another ethical issue is the commercial use of user's personal data i.e. the selling of personal data to ad companies. The data collected by the app might be used by ad companies to try and provide their idea of relevant ads which may not really reflect the users' needs. For example, if the fitness track records that the user likes to consume a certain product e.g. chocolate, and the advert company gets this information, it might target the users with chocolate ads which in this case are not what the user wants since they used the application to try and regulate their chocolate consumption, a process which to do, the fitness tracker has to be tracking their diet and recommending healthy options.

This will not benefit the user since they may be trapped in a repetitive cycle of conflicting recommendations namely of healthy diet and chocolate ads, a cycle which though potentially disadvantageous to the user, will nonetheless be benefitting the ad company and the application creator.

The issue at hand is closely related to that of whether companies should be allowed to use data collected to advertise their products without the consent of the user. This will violate the user's privacy rights which will heavily affect the user. An example of this is when Targets Artificial Intelligence algorithm figured out that a girl was pregnant before her father was aware (Hill, 2012). Target then started sending ads for pregnant women to her mailbox. When her father saw these mails, he protested on why Target was encouraging her daughter to get pregnant, a situation which to his surprise, later discovered to in fact be true.

Another potential professional issue that might arise in this application is receiving wrong health advice due to the sensors recording the wrong data, the GIGO (Garbage In Garbage Out) scenario, and thus leading to the application giving wrong suggestions or advice. The application does not record the user's hospital records or the user's allergies and this can lead to the application suggesting solutions not based on substantial medical data. This can be harmful to the user, consequently forcing the user to quit using the application which might heavily impact the company's finance and reputation especially if the user makes a public review.

In addition, if the user possibly follows the unreliable suggestions, they may end up being hospitalized. This may lead to the company being fined or the person responsible receiving jail time if the impact on the user is severely injurious. A person's health is a crucial field to get invested in since any malfunctions in the technology system being used might lead to fatal consequences. An example is the use of robotic systems to perform surgery, a method whose consequent concerns included the Da Vinci Surgical systems being linked to 144 deaths in the USA (BBC, 2015).

This project targets a very significant field which is a person's health implying that just entrusting any new and untested technology is unethical. For certainty on the project, it would have to be tested on real human participants which also presents an ethical issue. In addition, trained professionals in a certain field tend to face difficulties when using new technologies different from what they are used to which occasionally carries fatal reprecussions. For instance, the case with Newcastle's Freeman Hospital and their robotics heart programme with the Da Vinci Robot which led to the death of a patient, which would have otherwise been avoided had it been done conventionally with the low risk procedure, in which the patient would've had a 98.99% survival expectation (Donald & O'Brien, 2018). Furthermore, many users would find it hard to trust an application on their smartphone than advice from a trained professional which may also be a hindrance to the project.

References

BBC. (2015, July 22). *Robotic surgery linked to 144 deaths in the US*. (BBC News) Retrieved November 6, 2019, from bbc.co.uk: https://www.bbc.co.uk/news/technology-33609495

Chapman, M., Anderson, M., & Bajak, F. (2018, December 1). *Risks from stolen Marriott data: espionage, ID theft, home burglaries*. Retrieved November 4, 2019, from The Mercury News: https://www.mercurynews.com/2018/12/01/risks-from-stolen-marriott-data-espionage-id-theft-home-burglaries/

Donald, K., & O'Brien, Z. (2018, November 8). *Coroner says decision to use robot in UK-first heart op led to patient's death as it emerges blundering surgeon now has new job at another hospital*. Retrieved November 6, 2019, from https://www.dailymail.co.uk: https://www.dailymail.co.uk/news/article-6367481/Patient-died-robot-used-heart-op-surgeon-99-chance-surviving.html

Hill, K. (2012, February 16). *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*. Retrieved November 3, 2019, from Forbes: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/

Information Commissioner's Office. (2018, May 25). *Guide to the General Data Protection Regulation.* Retrieved November 3, 2019, from https://www.gov.uk/: https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation

legislation.gov.uk. (1984). *Data Protection Act 1984*. Retrieved November 3, 2019, from http://www.legislation.gov.uk/: http://www.legislation.gov.uk/ukpga/1984/35/contents/enacted

legislation.gov.uk. (1998). *Data Protection Act 1998*. Retrieved November 3, 2019, from http://www.legislation.gov.uk/: http://www.legislation.gov.uk/ukpga/1998/29/contents

Sweney, M. (2019, July 8). *BA faces £183m fine over passenger data breach*. Retrieved November 4, 2019, from The Guardian: https://www.theguardian.com/business/2019/jul/08/ba-fine-customer-data-breach-british-airways