The Use of Privacy Data by Fitness Applications, a User Point of View

Robin Leijdekkers(s1350455)
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands

ABSTRACT, In a world where smartphones have an important role in society, for almost everything there is an application to download. In the health section of application stores there are numerous fitness apps to download and use. These apps are popular to independent amateur athletes but do use a great amount of privacy information of users, called privacy data. This thesis examines the opinion of fitness application users about the use of privacy data. The choice is made to first analyze available literature about privacy violations in smartphone (fitness) apps. Hypotheses were derived from this literature and tested on the basis of interviews performed to sketch users' opinions on this matter. Theories about privacy data use of applications and interview results were compared to come with two interesting conclusions. Our research points out that users have a negative perception about privacy violations due to fitness applications. However, this perception is not turned in to action; users do not change their app usage. This would mean that developers of fitness apps do not have to deal with negative consequences due to their data collecting applications.

Supervisors: A.A.M. Spil

Keywords
Smartphones, fitness apps, users, privacy, data, literature, theories, interviews, app developers

5th IBA Bachelor Thesis Conference, July 2nd, 2015, Enschede, The Netherlands.

1.INTRODUCTION

In this modern society where nearly a quarter of all human beings on the planet is in possession of a smartphone (Curtis, 2014) there are subsequently millions of downloadable applications. Because of the extensive growth of the smartphone market and its possibilities, currently everyday the big application markets (like Google's Play Store for smartphones with Android-software and Apple's App Store for all Apple smartphones) bring us tons of new applications to download and use. For example, it was recently reported that the IOS AppStore has more than 1000K apps and more than 10 billion downloads (Blog.Appfigures, 2014). Furthermore, the appearance of tablets and mobile devices with other form factors, which also use these marketplaces, has increased the diversity in apps and their user population. Applications have become very important in our lives. Hence, they are integrated in the most important aspects of our lives. Health is such an important aspect and smartphone applications are an important part of serious gaming in health. People that like to sport and exercise for better health can find many applications that provide them with help and assistance. App-developers provide smartphone users with apps that for example track how much exercise is done and how much calories have been burned. Specific running apps track where, when and how long a user has been running in a single session. Naturally, every app has its own special features like heartbeat monitoring or music integration (Pappas, 2014). The numbers of downloaded fitness and running applications show that these applications are popular (Khalaf, 2014). People use these fitness and running applications especially to retrieve useful information about their exercises or sport sessions. To gain access to this information, many of these apps ask the user to fill in information about them selves. It could be well possible that developers make these apps to gain private information. Information about the user could include the user's age, weight, height, address and email. In many cases this data is not only used by the app to deliver the information that the user expects form the app. According to Linda Ackerman (2013) many fitness and running applications use this information for commercial purposes. Research made clear that many applications use the information of the users without permission. Researchers warn that a surprisingly high percentage of all available applications threaten your privacy. For example, joint research by Intel Labs, Penn State and Duke University found that 15 out of 30 Android apps analysed sent geographic information to remote ad servers without users' knowledge (Gralla, Sacco & Faas, 2011). On top of that, Ackerman stated:

''Our research brought us to the conclusion that, from a privacy perspective, mobile health and fitness applications are not particularly safe when it comes to protecting users' privacy.''(Ackerman, 2013)

Applications send the information to the developers, who are happy to use this information for commercial ends. The Nike+ running app is one of those applications that gathers privacy data and sends it to Nike, who uses this information for the promotion of their products (Schneier, 2006). There are also many applications (like Fitness Pro and Runkeeper) that are not directly in contact with other companies like Nike. That does not mean that these apps do not use information of the users. Many fitness and running applications send privacy data of users to interested organizations (for example manufacturers of sportswear like Nike):

'*Meanwhile, in June 2010, security vendor SMobile Systems found that 20% of Android apps allowed third parties (that is, companies other than the app vendors themselves) to get access to private or sensitive information.''*(Gralla, Sacco & Faas, 2011)

Organizations that are interested in the collected data are often willing to pay big money to the developers of the applications (Yildrim, 2012). This can all take place without permission of the relevant users. Without knowing usernames, email addresses, zip codes, geolocations, contacts, gender but also maybe even eating habits and weight data are being send to third parties who could benefit from it. More and more people became aware of this matter the past years. It could be interesting to find out whether users think this matter is a problem and therefore say use of privacy data without permission by fitness and running apps is unacceptable. There could be a lot of users who think it is very important to maintain their privacy, especially in a time where information can be gathered and exchanged quicker as ever before. People are not aware of how much information can be found about them on the Internet (Wetherall et al., 2013). It could be interesting how people think of this when personal information is retrieved by a fitness application. It is also possible that fitness and running app users are not negative about this matter. For a matter of fact there are many users of fitness and running apps that like to share their performances and results achieved with the app to friends. Do these people care less about the usage of their privacy data?

Hence, I think it is interesting to do research about this subject because application developers and organizations that are collecting privacy data could use benefit from the results. Especially when it is about fitness and running applications, much sensitive privacy data can be derived from users compared to other applications. Fitness and running applications ask much information of users and these apps do very often use location services and they always want to know what the location of the user is.

When it is about gathering and forwarding of personal data without users' permission, people could react detached and could want to avoid these kinds of applications. This is something application developers probably do not want; how bigger the number of application users, the greater the profits. Therefore, I think that it could be relevant for these organizations to know to what extend the users have a negative perception about it. Hence, maybe these organizations will think differently about the use of privacy data and thus want to change something about their business model. Moreover, it could also be interesting because there has not been much research on this subject;

''Despite the popularity and potential of health and fitness apps to assist individuals in leading a healthy lifestyle, research related to the design of such apps is limited.'' (Yoganathan& Kajanan, 2013)

1.1 Problem Statement

As stated before, nowadays it is quite common that applications for mobile phones make use of the data of the users to benefit from it financially:

''*Ensuring that the flow of sensitive data through apps to remote servers does not violate a user's privacy is an important and difficult problem.'' (*Gilbert, Chun, Cox & Jun, 2013)

From a user point of view, fitness applications should be helping and stimulation people with exercise. However, fitness applications are part of a group of apps that asks users for their data, like location details with the GPS-function of a smartphone. Applications can use privacy data directly but it is also possible that applications send data to third parties. This fact is not clear to all users of fitness apps but the general awareness is increasing. On top of that, the opinion of the particular users of fitness apps is not quite clear although this issue is treated as a problem. I think this opinion could be useful for application developers and organizations that make use of privacy data. When people unanimously disapprove this state of affairs the problem could become more relevant to developers of fitness applications. What if people decide not to use fitness apps anymore because they do not want their privacy data to be spread? The purpose of this research is to find out whether users of fitness and running apps reject the use of privacy data and to give relevant organizations like application developers advice on the basis of this outcome. Maybe even more important: what does a positive or negative perception mean for the continuity of the usage of such applications?

1.2 Research Question

When summarizing the problem statement: The use of privacy data by fitness apps is a touchy subject in the literature. However, it is not clear what the users of these apps think of this issue and how important they think their privacy is. The following research question is formulated:

''To what extent do users of fitness apps have problems with the use of privacy data by application developers?''

The main research question can be split in to a few other relevant sub questions:

- What is privacy and what are fitness apps?
- How big is the share of fitness apps that use privacy data?
- How important is privacy for users of fitness apps?
- To what extent are users of fitness apps aware of the use of privacy data?
- To what extend do fitness applications warn users for usage of privacy data?
- What does the awareness of the users mean to the usage of fitness apps?

2. RESEARCH METHODS

For this research, I will perform a literature review and I will analyze existing interviews to answer the main research questions and the sub questions.

2.1 Literature Review

First of all, I will try to answer the sub questions by analyzing existing literature and when this is done, I will come up with hypotheses, derived from the literature. These hypotheses are in fact a set of statements that can be formulated by making conclusions on the basis of the facts given in the found literature. After formulating hypotheses, I will try to test the hypotheses with the answers existing interviews. The interview method is explained in the next paragraph. When I have a clear view of people's opinions about this matter, I will try to link this view to existing literature about the usage of privacy data by applications and come with conclusions. It is my purpose to find out more about how applications derive privacy data from users and to what extent this happens. I also analyzed several papers about privacy violations in app usage, and not only in fitness applications. Privacy violations are logically also an issue in other apps. This method has provided me with a good indication of the current situation about privacy in fitness applications and other applications. To perform this literature review, two large databases were used to retrieve several relevant scientific papers about the subject, named Google Scholar and Scopus. To search for relevant scientific papers, some accurate key words were needed to search through the databases. For this search for terms like: (fitness) applications privacy data', ' (fitness) applications privacy policies', 'smartphone applications privacy information', 'Smartphone users privacy awareness', 'privacy policies smartphone applications', 'Smartphone fitness applications, 'privacy data', warning users (fitness) applications privacy' and ' importance privacy (fitness) applications' were used. With the hits I had on these search terms, both databases provided me with a great number of papers that seemed relevant on first sight. To keep this research as relevant as possible, all the literature about applications and privacy aspects to from before the year 2012 were discarded to keep the research as recent as possible. To deal with a feasible amount of literature, they were analyzed on their relevance. Of most of the papers, the abstract part of the papers indicated whether it could be considered as relevant of not. Due to this method, I ended up with a select group of relevant studies. Most of the research papers I found in the databases discussed privacy issues of smartphone applications in general, but some of them specifically discussed fitness applications.

2.2 Interviews

As I discussed earlier, several hypotheses were derived from the relevant literature I found in order to answer the sub questions. After this, my purpose was to test the hypothesis on the basis of the analysis of available interviews. In May 2014, 41 people were interviewed about serious gaming in health. The interviews were semi-structured. According to Fontana & Frey (2000) this is an incomplete interview script where the researcher may have prepared some questions before hand, but there is room for improvisation. The interviews took place in the Netherlands at the University of Twente. All participants were Dutch and they were asked about their opinion about the usage and characteristics of fitness and health applications or games. To analyze the interviews, we used the theory of Miles & Huberman (1994) for qualitative analysis. According to them, the first step of performing qualitative analysis is to data reduction. With this step, discarding all irrelevant data is important. All data considered unnecessary has to be discarded, but making sure to keep the discarded data accessible for unexpected findings could be wise. Among our interview questions, there were several questions that were interesting for this research, like questions about privacy data usage and which personal information they were willing to share with the application. However, not all participants of the interviews were users of fitness applications in specific. Four out of 41 participants were users of Wii fit, a fitness expansion for the Nintendo Wii game console. These participants are left out of this research because we specifically discuss fitness applications (on smartphones). In addition to this, 14 of the 41 participants discussed health apps that are connected with their personal health record and personal physician. These apps cannot really be seen as fitness applications because these have more health record characteristics, instead of apps that are used for physical activities like fitness apps. The interviews of these 14 participants are also not used for this paper. Besides these interviews that were not usable, there was one more participant

that did not discuss a serious health game at all. Naturally, this interview was also not relevant. Therefore, there were 22 interviews with participants left that discussed fitness applications in specific. Of these participants, one was younger than 18 years old, 20 were between the age of 15 and 35 and two were older than 45. For this research I especially analyzed the group of participant aged between 18 and 35 to deal with the biggest group. All participant of this group have HBO or VWO (collage or University) as highest form of education. In addition, not all interview questions were relevant because not all of them were about privacy aspects of the application. The second step given by Miles & Huberman (1994) is to present the received data graphically; to draw conclusions from the mass of data, they suggest a good display of data. Subsequently, with the interviews of these 19 participants I tested the hypotheses I derived from the literature and I tried to indicate if there was a pattern in the answers the participants gave. This is done to address Miles & Huberman's third and last step, drawing conclusions. In other words, I looked for answers that indicate users' perceptions on the matter of privacy violations in the usage of fitness apps. This done on the basis of quoting the answers of several participants and giving some quantitative information about the interview outcomes in graphics.

3. LITERATURE REVIEW

In this part of my research paper I will try to answer the sub questions with existing literature. For some sub questions there is not much information to be found on fitness apps in particular, but there is much to find about apps in general and their aspects of privacy. For this paper, I consider fitness applications on smartphones as part of smartphone applications in general. By this I mean that most of the aspects of apps in general that are being discussed also apply to fitness applications. Logically, users of fitness applications are also user of other apps and they see a fitness application as part of their app collection.

3.1 What are Fitness Apps and what is data Privacy?

This research examines people's opinion about privacy data usage of fitness applications. First of all, it is important to clarify what fitness applications are and what they are not. Privacy Rights Clearinghouse (2014) considers fitness and health applications as what we consider as wellness apps, for consumer use (Privacy Rights Clearinghouse, 2014). They do not focus on applications that integrate with medical treatment or are intended for medical treatment for professionals. In the research of Privacy Rights Clearinghouse these apps can be interactive but also informational. Customers can 'participate' in an application, but the other apps can also be used to look up information about diseases, medications or horoscopes for example. David Gilles (2014) defines fitness apps as 'software programs that help you achieve and maintain a sound mind, body and spirit'. According to him, heart rate checkers, calorie counters and weight loss indicators are popular features of these apps. In this research paper, the focus is fully on interactive fitness applications, used to assist people with physical exercises and keeping them in shape, especially because these smartphone applications do ask much private information of their users. These applications are known as intensive users of personal data like name, age, height, weight and eating habits, to highlight some examples. This information is used to give the user the best experience of the app and to help the user to be as productive as possible. One of the features of these kinds of fitness applications is often tracking the exercises of the user by location. Applications like Runkeeper, a running application, gives the user the opportunity to track the duration, distance and route of a single running session by using the GPS function on a smartphone. Another reason why fitness applications in specific are interesting to look at, when speaking of using privacy data, is because these apps depend on advertising to make money. They may share personally identifiable information with advertiser, or allow ad networks to track you. If an application collects your device id or embeds a unique ID in the applications you download, de-identified analytics data can be tracked back to you personally (Aditya, Bhattacharjee, Druschel, Erdélyi, & Lentz, 2014) Subsequently it is also a fact that many mobile fitness applications have poor security. Although they may have a privacy policy that says they protect the privacy and confidentiality of your information, more often than not, they transmit it unencrypted and over insecure network connections (Agrawal, Sodhi & Probhakar, 2013). Downloading these applications can be done by going to the website of developers and Amazon has also a large selection. It is much easier and most common to the AppStore for IOS and Google Play for Android. Here you can search by app name or type and you can read about the app before downloading it. If the fitness applications also have a privacy policy you can often find prior to the download. If you cannot find it, it is possible that there is no website or privacy policy for a specific application.

When speaking of the opinion of users about the privacy data of fitness apps, it could also be useful to give a definition of in app privacy. I mentioned a few examples of personal data like name, weight and location. When others than the users find or collect this personal data, this is considered as an invasion of privacy; some other company or group of people gets to know their personal information. When taking a look at a broader, more common definition of privacy, 'the right to be let alone' is a general explanation. Louis Brandeis and Samuel Warren (1890) formulated this interpretation in their groundbreaking paper on privacy. This paper recognizes that each person has a sphere of existence and activity that properly belongs to that individual alone, where he or she should be free of constraint, and even uninvited observation. According to this paper, each of us needs our own space. However, in this paper I only deal with data privacy, a much narrower meaning of privacy. This narrower meaning of privacy, which James H. Moor (1997) calls information privacy, that concerns us here, because that is what is threatened by information-processing capabilities of computers (Moor, 1997). He defines the right to informational privacy as the right to control of access to personal information'. This is a common definition in the literature and it contains four important elements. First Information. This focuses on the quest for knowledge about someone, rather than for example physical proximity or constraint, or any type of interference. Second, it refers to personal information. The knowledge intended gives some access to the subject's person, whether it is his or her identity, habits, weight or length. The third element is control. In this matter, it is not about how much and how little is known about someone, but whether the subject can choose how much information is revealed and to whom. The fourth element is about the fact that privacy is defined as a right. Within certain domains, the person's control of personal information ought to be respected and protected. The information Moor gives us is more relevant to our research because of course in this paper we focus on the data applications derive from users. This data is logically informational data.

3.2 How Big is the Share of Fitness Apps that use Privacy Data?

When looking at the second sub question, we will try to clarify to what extent all applications collect privacy data. Craig Michael Lie Njie(2013) investigated 43 popular mobile health and fitness apps and came with some interesting conclusions. He investigated the data flow of these selected applications. Of these 43 fitness and health apps, half of them were paid en the other half was free to download. There was also a distribution of where the applications were downloaded from: half was from IOS and half from Android. The results are placed in Table 1. In addition to this information, Nije noticed that apps with the most detailed privacy policies posed some of the greatest privacy risks. All this information derived from Njie's work indicated that a high degree of the selected apps do use personal information and send often send it to third parties. The percentages found by Njie indicate that the usage of privacy data by fitness apps is an issue. Other literature and our interviews will have to point out whether it is a unwelcome issue to the users of the fitness apps or not.

Table 1. 43 health and fitness apps analyzed on privacy data usage (Nije, 2013)

Percentage of analyzed apps that used some kind of behavioral tracking, often through multiple third party analytics	Free Apps: **75%**	Paid Apps: **45%**
Percentage of the analyzed free apps that used some kind of third party advertising. Send usage data to as many as ten or more different third party advertisers in the firs few minutes the app is in use.	Free Apps: **47%**	
Percentage of analyzed apps that send data to the developer	Free Apps: **78%**	Paid Apps: **40%**
Percentage of analyzed apps that send data to third-party sites as part of their core functions	Free Apps: **52%**	Paid Apps: **40%**
Percentage of analyzed free apps that store data on local device	Free Apps: **83%**	
Percentage of the analyzed free apps that store cookies and other identifiers locally on the device	Free Apps **79%**	
Percentages of analyzed apps that were divined as 'high risk' and 'medium risk'	High Risk: **40%**	Medium Risk: **32%**
Percentage of analyzed apps that posted a privacy policy and adhered to it	Free and Paid Apps **50%**	

3.3 Is Privacy Important to the Users of Fitness Apps?

The previous part of this literature study triggers another sub question; 'is privacy important to the users of fitness applications?' To answer this question by looking at existing research is difficult, because there has not yet been much research about the opinion of people about these specific applications. However, there is something to find about the opinion on privacy data usage of apps in general. For example it is a fact that second to only battery life, privacy is one of today's smartphone user's top concerns on their devices (Deasy, 2013). Despite the high demand for free ad-driven apps, 43% of users in the US and 47% in the UK are not willing to share personal information with a company in exchange for a free application. Another study indicates that the willingness of users to share their age, full name, date of birth and web-surfing behavior decreased the past years. Interestingly, this research made also clear that customers are more protective about their contacts than their home address, phone number or current location. The same report also showed that smartphone users are more concerned about their mobile privacy than the device brand, camera resolution or the device's weight. Another study by Jorgensen, Li, Chen, Proctor, Gates and Yu (2014) asked users what risks where of their greatest concern. When downloading a new application on their phone., users showed the most concern for information privacy risks, followed by data integrity, eavesdropping/spying, device instability, spam, monetary risks and finally, physical device damage (Jorgensen et al., 2014). This shows that when speaking of risks on a smartphone, users see privacy threats as a great problem. Besides of these facts, there are more reports and surveys that point out that this matter of mobile privacy is considered as a problem for the users when asked.. We can conclude that keeping their personal information private is important for app users.

3.4 Do fitness Apps Warn Users for their Usage of Privacy Data?

Another important subject to look at is whether fitness applications warn users for the usage of their personal information. Let us consider that when apps warn users for specific attributes of the app, this has to be done by attaching privacy policies application developers linked to their app. A study by Sunyaev (2014) gives us some other facts about the privacy policies of health apps in specific. Of the 600 most common used applications about 30 percent had privacy policies and the average length of these privacy policies was 1755 words. Two third of the privacy policies did not specifically address the app itself. Sunyaev draws the conclusion that his findings show that developers of health applications often fail to provide privacy policies. The privacy policies that are available do not make information privacy practices transparent to users, require college-level literacy and are often not focused on the app itself (Sunyaev, 2014). Another study in 2014 gives us some more facts and numbers of the privacy policies of fitness applications in specific. It indicated that about 43 percent of all free health and fitness apps have a link to the website of the privacy policy in addition to 25 percent of all paid apps in this category. This study also shows that 48 percent of all free apps with a privacy policy in this category have a privacy policy that does not apply to third party links. For the paid applications this was 25 percent. 57 percent of the applications with a privacy policy notify the users that personal information made public is not protected. This applies to 15 percent of the paid applications (Privacy Rights

Clearinghouse, 2014) To sum op this literature about warning users about privacy data usage of applications, we see that when focusing on applications in general, just about half of the available apps deliver a privacy policy to inform the users about the properties of the app. Besides that there is such a great margin of applications that do not deliver a privacy policy, the applications with a privacy policy do not always have an accurate one. This means that half of the privacy policies do not even describe the actual activities of the app. The more specific facts on privacy policies of health and fitness apps show that also in this category they lack of accuracy on the real activities of the apps. There is a slight difference between the policies of paid applications and free applications, logically those of the paid apps are more accurate and provide more information.

3.5 Are Users of Fitness Apps Aware of the Use of Privacy Data by Fitness Apps?

It is also interesting to see whether users of mobile phone applications are aware of the things they do. This research aims to divine the opinion of users about privacy usage of fitness apps, but do these users even know about the fact that applications have these functions? Therefore, it could be wise to indicate how users of apps in general perceive security and privacy risks created by mobile apps. A survey with more than 6000 participants in nine markets around the world showed some interesting facts. For example, one in four respondents was not aware that apps can modify browser bookmarks, access the phone's camera and microphone, or send photos to the developer. Even half of all respondents in all regions were unaware that apps can send physical location details. (Rosch, 2014) A study performed by El Hadadi& Shidhani (2013) also shows us that a very large part of all smartphone users are not aware of how applications can harm their privacy and security. For example, more than half of the respondents of their survey did not have a clue on issues related to smartphone security and security best practices. Procedures such as performing updates, awareness on certain applications and following safe measures in using smartphones were not of their concern (El Hadadi & Shidhani, 2014). El Hadadi & Shidhani end their study by concluding that more awareness campaigns for users are required. When looking at our sub question, we can conclude that there is much left to be desired, speaking of awareness of activities of applications that can violate privacy. A large part of the smartphone users does not know much about privacy issues in applications, despite the increasing threats as smartphones host more processing powers and memory banks. We consider that this fact also applies to the users of fitness applications.

3.6 What Does the Awareness of the Users mean for Their Usage of the Fitness Apps?

Considering the other part of the smartphone users does know about the possibility that applications use personal data, it is interesting to find out what their reaction is. How will users act when they are aware of the negative activities of these apps? A study performed by Boyles, Smith & Madden (2012) indicates that more than half of (aware) app users have uninstalled or avoided an app due to concerns about personal information. To be more precise: 54 Percent of app users have decided to not install a smartphone app when they discovered how much personal information they would need to share in order to use it. 30 Percent of the users have uninstalled an app that was already on their phone because they learned it was collecting personal data that they did not wish to share. Owners of both Android and IPhone devices are equally likely do delete or avoid smartphone apps due to concerns of their personal data (Boyles, Smith & Madden, 2012). These facts point out that when users are aware of what information the applications use, the chance is quite big that he or she chooses not to use the app anymore. This does not mean that the other people that are aware of the activities of some apps choose to do nothing about it. On this point, another interesting fact is that one in five (20 percent) smartphone users have turned off the location-tracking feature on their phone because they were concerned that other individuals or companies could access that information. This measure is an alternative for choosing not to use these applications. We can conclude that a large part of the smartphones users is willing to take action to protect him or her self when aware of the privacy violating activities of an application. However, when speaking of fitness applications, often turning off the location tracking is not an option, because many fitness applications have this as one of the most important functions of the application. Of course, it is possible not to use the applications or to delete it to protect your self from the possible negative activities of the app.

4.HYPOTHESES

Based on the literature study part of this research paper I will now formulate four hypotheses focused on the main research question: To what extent do users of fitness apps have problems with the use of privacy data by application developers?

First of all, the literature that we found made it quite clear that smartphone users are not always aware of what applications do with personal data. Half of the respondents of a survey performed by Rosch(2014) seemed to be not aware of the fact that smartphones can send physical location details. One in four participants was not aware of other privacy threatening activities that applications are capable of on their smartphones. I wonder to what extent this can be seen in the interviews, to what extent users know what smartphone applications are capable of and if they know the possible dangers. Our first hypothesis:

H1: Users of fitness applications are not always aware of the privacy data usage of the applications.

The literature also made clear that the privacy is very important to smartphone users and it is seen as the biggest risk when using a smartphone. Jorgensen et al. (2014) found out that smartphone users showed most concern for privacy risks when speaking of possible risks in smartphone users. This means that these smartphone users are negative about privacy threats. From this point, users can be seen as suspicious, but we also indicated that not all users are aware of the risks. When they are aware of the risks and are suspicious, it seems obvious that users act careful when they select the personal information they want to share. That makes it interesting what the interview results tell us. Our second hypothesis:

H2: When users of fitness apps are aware of privacy data usage, they are negative about it.

According to the research of Deasy(2013) users have become more cautious in sharing their personal information with smartphone applications the past years. His research pointed out that almost half of the people he asked were not willing to share their personal information in exchange for using a free application. Privacy is an issue that users are very concerned about according to the same research, so part of those users will decide not to give the application the data they demand. Thus, when we take a look at our interviews, we will expect that part of the interviewed users will declare that they will not share some specific information. Our third hypothesis:

H3: The privacy aspect is very important for the users of applications, and therefore the questioned users will not be willing to share their personal information with the app.

Another point made clear by the literature is the one that indicates that users who are aware of activities of an app when it comes to handling personal data, they will try to stop these activities or just stop using the application. Boyles, Smith & Madden (2012) indicated that more than half of the questioned smartphones users uninstalled or avoided an app due to concerns about privacy threats. In addition, 20 percent of the participants in their study turned off the location-tracking feature of their phone because they were worried that other individuals or companies could access information about their home location.. This study made it quite clear that some of the smartphone users take measures to prevent applications to use their personal information. Will the interviewed users of fitness applications show the same phenomenon? Our fourth hypothesis:

H4: When users know that personal information is shared by the application in use, they will try to do something about it or stop using the application.

5. DATA COLLECTION

The interviews that were performed in May 2015 gave us an indication of the opinion of users of fitness apps about privacy data usage. As stated earlier, the received data is presented and analyzed using the theorie of Miles & Huberman (1994). As stated earlier, 22 participants used a fitness application on their smartphone, 20 of them were between 15 and 35 years old and three of them were older. I have decided to only deal with the first group to keep a large number of participants. The interviews consisted of several questions about their usage of the applications. The interviews for instance had to make clear why they used fitness applications, how they use it and where they used it. Questions that were relevant for this research, questions about privacy matters of application usage, were also asked. For example the interview consisted of questions about which personal information users wanted to share with the application and whether they think the application provided them reliability and privacy. In addition there was a specific question about whether the users think that their privacy is at stake due to the applications or not. The participants had to tell whether they think their personal information could fall in to other hands. In this part of our research we will analyze the interview results. We will tried to look for prominent patterns and answers that we will compare with the hypothesis in the next chapter of the research. Some striking and relevant quotations of the respondents were used to illustrate specific findings. First, we will take a look at what personal information users were willing to share according to the interviews. The interviews distinguish three different types of personal data that users are going to have to share with a fitness application. These types of personal information are: body information (like heartbeat, length and weight), habits (like eating, smoking, exercising) and environment (like work and home location). The participants could indicate at each type just whether they would share the information or not. This gave us the following results:

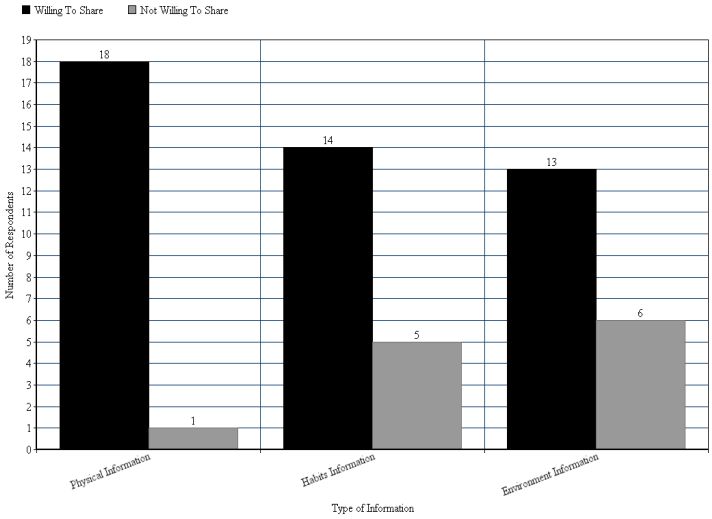

Figure 1. The willingness of users to share personal information

As we can see in figure 2, most of the participants are willing to share all information. There was only one participant that was not willing to share his physical data; there were 5 not willing to share habit information and 6 not willing to share environment information. This could mean that information about user's locations is seen as most valuable, followed by information about habits and physical information. However, some of the participants that stated that they were willing to share all types of information under the condition that the given information was made anonymous or remained private. Out of 13 participants that were willing to share all types of information, eight were willing to share the information with the fitness app under these conditions. These people were not aware of what the fitness applications are capable of in using privacy data. One of the participants said:

''I am willing to share everything with the application, but only when it is safe and people can not find this information on the internet. I am using a password on my smartphone so other people can not see the information on it''

This statement indicates that this user is most likely not fully aware of the capacities of the fitness application. The user is not aware of the fact that applications can derive information from smartphones without putting it on the Internet. Using a password is effective to prevent your private date from people in your surroundings, but naturally this does not stop applications from collection personal information. Another participant said the following:

''The amount of information that I wish to share depends on whether the data is kept anonymously or not. When this is the case, I am willing to share the data. I have to say that when I am using a smartphone I am more prepared to share my personal data than when I am using my computer, because I think the computer is more dangerous for my privacy data.''

This quotation indicates that this user is suspicious when it comes to sharing personal information because he wants to share the data anonymously. However, the participant says he is

more comfortable with sharing personal information with apps on his phone, than on his computer. It is not really clear whether the participant is aware of what applications are capable of when it comes to collecting personal data of users. There were also participants that were willing to share all their personal information unconditionally. One of them said:

''I am willing to share all the information, because in that way the app works most effective for me''

This statement indicates the opinion of a user that does not seem to care about what happens with the personal information, or the user is just not aware of the fact that many apps collect the information to use it.

Another question in the interview was about whether users of fitness applications think they provided them reliability and privacy. The answers from the interview show that the participants do not seem to worry about the reliability of the service the fitness application provide. However, when asked about whether they think the application provided them privacy the answers showed more variance. Eight out of 19 participants trusted the fitness application when it comes to privacy. The reason for this opinion can be that these participants are not aware of the activities of the app on this matter, or that they are sure about the fact that the application does not use and send their personal data to third parties. When we look closer to the arguments of these eight participants, we see that all of these participants just assume their privacy data is safe by sharing it with the applications. These participants gave answers like:

''Yes, I think the application is safe when it comes to privacy data. I have a password on my phone so no one else can see my personal information.''

This participant thinks that a password on her smartphone prevents others to see the personal data she gave to the application. It seems that the participant is not aware of the fact that applications are able to collect the data and a password does not prevent this. Another participant said:

''I am convinced that the application treats my personal information in a proper way.''

This participant thinks that the application does not use the other purposes than the core activities of the application. Maybe this respondent is also not aware of the fact that many fitness applications do collect privacy data for other purposes.

The other 11 participants thought that the fitness application they use did not provide them privacy, or they were not entirely sure about it. The answers of these participants showed much similarities; these participants seemed all aware, or cautious about the fact that fitness applications are capable of collecting privacy data to use it for other purposes. A statement from a respondent that confirms this:

''I am very skeptical about privacy usage, especially nowadays where no one seems to have any privacy. I think that your personal data is not safe when using smartphone applications''

Another relevant question in the interview asked the participants about whether they thought if they shared their personal data with the fitness application, it could fall into other hands,. With ''other hands'' we mean the possibility that the personal information could end up at third parties that collect data for promotional activities. When we took a look at the interview results of this question we see that 10 out of 19 participants thought that their personal data could end up in the hands of others. Seven respondents indicated that this was probably not possible and two respondents had no clue about whether fitness applications were capable of sending their personal data to others (see figure 2.)

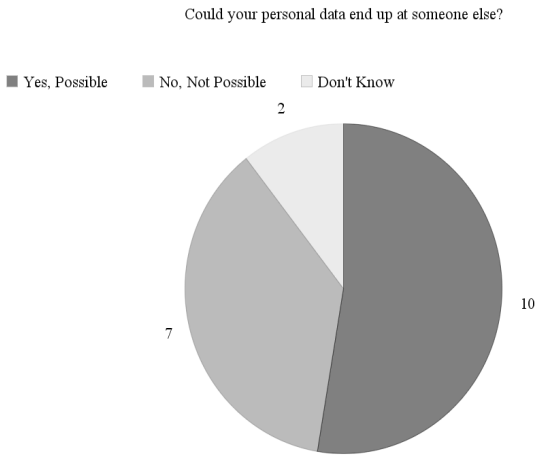

Figure 2. Users' view on whether their personal data could end up

The respondents had also the opportunity to indicate whether they consider it as a problem or not, when their data is sent to other parties. Four out of all 19 participants indicated that they did not see it as a problem when their personal information is send to other parties. On of them states:

'' I think this could be possible. However, I would not have any problems with it.''

Even though, the other 15 fitness app users considered it as a problem when this happens to their personal data due to their usage of a fitness application. One of them answers:

''Like I said earlier, I am really afraid of the fact that this could happen to my privacy data. I am always afraid of others using my personal information.''

To summarize, the group that sees this matter as problem is much larger than the group that does not.

The final fact that the interviews indicated is that there was only one respondent that clearly indicated that here usage of the application depended on whether her personal information was save with the app or not;

''Yes, the possibility that other could collect and look into my personal information is for me the most important thing to look at in deciding whether to use the application or not.''

The other participants seemed not to change their behavior in using the application, despite the negative perception several users had towards the privacy aspects of the app.

6. DATA ANALYSIS

In this part of our research we will try to test the composed hypotheses by comparing them with the results of the interviews. After this comparing, we will draw some conclusions. In other words, we will look whether the participants of the interviews gave answers that confirm the hypotheses or not. A hypothesis could be in line with what the respondents had to say and thus be confirmed. Of course, there was also the possibility that the interview results were not in line with a hypothesis and had to be rejected. From these

comparisons we could draw some striking conclusions, which were relevant for answering the main research question.

The first hypothesis that we formulated was: *Users of fitness applications are not always aware of the privacy data usage of these apps.* This hypothesis was derived from the information from the research of Al Hadadi & Shidhani (2013) and Rosch (2014) provided us. Both indicated that many users are not aware of the activities and capabilities of apps when it comes to collecting privacy data.

First of all, it can be said that the interviews point out that not every interviewed user was aware of the activities of the fitness apps involving personal data. From the statements of several participants can be concluded that not everyone knew that their personal data was not safe when shared with the app. Other statements made clear that some participants did not know what applications were capable of. For example, two participants seemed to be convinced that because of the fact that they used a password on their smartphone, no one else could collect their personal information. Other participants stated that is just 'not possible'. On the other hand, most participants seemed to be aware of the possible dangers of sharing personal information with an app, but the fact is that a part of them is not. The hypothesis can be confirmed.

The next step is to find out whether the participants that were aware of personal data usage by fitness applications have a negative perception about it. To repeat the second hypothesis: *When users of fitness apps are aware of privacy data usage, they are negative about it.* We came to this hypothesis by analyzing the work of Jorgensen et al. (2014). This showed that privacy threats are often the biggest concerns of app users, which indicates that they have a negative attitude towards it.

This hypothesis can mostly be confirmed. There are a few participants that explicitly indicated that they did not see it as a problem when their personal data collected by others. However, the vast majority of the participants seemed to worry about the fact that this could happen to their data. Several participants of this majority indicated that they are careful and suspicious when it comes to sharing their personal information with a fitness application. There were even some respondents that literally said that they were skeptical about applications using their personal data. Respondent's words like ''afraid'' and ''not safe'' also indicate that most of them are not comfortable with what can happen with their info. Clearly most of the participants saw it this way and therefore, the hypothesis is mostly confirmed.

The next hypothesis that will be checked is the one about the willingness to share information with the application: *The privacy aspect is very important for the users of fitness applications and therefore the questioned users will not be willing to share their personal information with the app.* By looking at the work of Deasy (2013) we came to this hypothesis. His work indicated that a large amount of users were not willing to share their personal information in exchange for using a free app.

The results of the interviews made it quite clear that the willingness to share data with a fitness app was great among the respondents. Only one of them refused to share all kinds of data (physical, habits and environment). The rest of the participants were all prepared to share at least some of the personal information. However, information about habits and locations seemed a bit less comfortable to share with a fitness app than physical information. After all, clearly the vast majority is willing to share their data with the fitness application and therefore our third hypothesis cannot be confirmed.

The fourth and last hypothesis to test was: *When users know personal information is shared by the application they will try to do something about it or stop using the application.* Thanks to the information Boyles,Smith & Madden (2012) provided us, we came to this hypothesis. Their research pointed out that many smartphone users tried to do something to protect their personal data from applications.

This hypothesis also cannot be confirmed. Only one of the participants clearly indicated that her use of the app depended on whether her personal data was safe and not used. The rest of the respondents seem not to change their behavior because of the apps' use of personal data, despite of their negative perception towards it. Most of them see this as a threat but it cannot be said that they are fighting or taking measures against this phenomenon. Thus, the final hypothesis cannot be confirmed.

7.CONCLUSION & RECOMMANDATION

After analyzing relevant literature about privacy data usage by (fitness) applications, we tested hypotheses by comparing them to the answers of an interview held on the subject about one year ago. Our main research problem will be answered, and also conclusions and recommendations will be given.

First of all, we can divide our main problem statement in two parts; first we had to make clear whether users had problems with the fact that their privacy could be violated due to a fitness application. Second, considering application developers, it could be relevant whether this attitude towards privacy violations in fitness apps is turned in to action or not. When answering the main problem statement; we can conclude that the interviewed users of fitness apps on their smartphones mostly have problems with the fact that their privacy data is not safe. However, not every respondent was aware of the capabilities of smartphone apps considering privacy data collecting. Most of these unaware users seemed to be convinced that their personal data was safe with the application, by using a password for example. They did not know that this does not keep applications from collecting personal data. However, from the answers of these unware users can be concluded that this group also has a negative attitude towards privacy violations by apps. The most interesting thing to see is that despite of the negative attitude of the respondents, most of them are not prepared to do something about it. Their usage of the applications is does not change. In contrast with what the existing literature (Boyles, Smith and Madden, 2012) states about users taking action in preventing their applications to use their personal data, the interviews indicate users keep using the app in the same way.

Developers of fitness applications should notice the fact that users often have a negative perception towards their applications when it comes to violations of privacy data. It could be wise for them to keep an eye on the developments of the reaction of users on this matter. Developers of fitness applications are often interested in large numbers of users, which affects their profits positively. Considering the outcomes of our research and the hypothesis testing, we can conclude that developers of fitness apps do not have to worry about the usage of their applications. The users do not seem to consider their negative perception towards privacy violations worse enough to change their application usage. Users see using the application as priority and therefore most of them do not take action. When developers of fitness applications consider our research results, this means that they do not have to change their business model in terms of collecting privacy data. However, it could be wise

for them to keep aware of negative users' attitudes towards applications that collect personal information.

8. LIMITATIONS & FURTHER RESEARCH

The results of both the literature review and the interviews show that users of fitness applications are not always aware of the dangers of data collecting smartphone applications. This raises the question why it is that not every smartphone user knows about the activities and capabilities of applications. In the literature part of this study paying attention to privacy policies of applications is mentioned as a possible way to make users more aware of application activities. However, we do not know how much influence ignoring privacy policies have on the overall awareness of users and to what extent this happens. It could also be interesting to look for more causes for unawareness of users about privacy data usage by (fitness) apps.

This thesis also focuses on how negative users are towards fitness applications and how this expresses in actions of prevention of the users. It could be interesting to explore this and ask users specifically on what their routine is before downloading an fitness application what their plan is to protect themselves from privacy violations. Maybe users have other ways to prevent other parties using their personal information.

The data collection part of this thesis consists of an interview held in 2014 and the results of 19 participants between 18 and 35 years old were used. This margin in age is relatively big and age could be a factor in explaining differences in answers between respondents. Maybe there are differences in awareness and opinion about privacy data usage of fitness applications between a 18 year-old and a 35 year old. Age could be a factor in a research on this subject because smartphones and applications is a relative new subject in our society. Nowadays children grow up with smartphones and that cannot be said about adults, who came in touch with smartphones on a higher age. Maybe age influences attitudes about the importance of keeping privacy and to what extent there is concern about it. For future research, there could be a comparison between opinions of different age groups about this matter.

It could also be interesting to do research like this again in a couple of years to analyze whether something has changed about the opinions of users on privacy data usage of fitness apps. Maybe there will be more regulations for applications developers in the coming years on this subject in and maybe there will be others events or situations that changes the opinion of users of fitness apps. Finally, it may also be wise to do research about this subject with interviewing a larger group and ask only specifically on the privacy aspect of using the application.

9. REFERENCES

Ackerman, S. (2013). *Mobile Health and Fitness Applications and Information Privacy*. [online] San Diego: Privacy Rights Clearinghouse, pp.10-23. Retrieved 18 May 2015 from: https://www.privacyrights.org/mobile-medical-apps-privacy-consumer-report.pdf.

Aditya, P., Bhattacharjee, B., Druschel, P., Erdélyi, V. and Lentz, M. (2014). Brave New World. *SIGMOBILE Mob. Comput. Commun. Rev.*, 18(3), pp.49-54.

Agrawal, A., Sodhi, B. and Prabhakar, T. (2013). A multi-dimensional measure for intrusion- The intrusive quality attribute. *Federated Events on Component-Based Software Engineering and Software Architecture*, [online] pp.63-68. Retrieved 26 May 2015 from: http://dl.acm.org/citation.cfm?id=2465497.

Al-Hadadi, M. and Shidhani, A. (2013). Smartphone Security Awareness: Time to Act. *Current Trends in information technology*, [online] pp.166-171. Retrieved 22 May 2015 from: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6749496&tag=1.

Blog.appfigures.com, (2015). *App Stores Growth Accelerates In 2014*. [online] Retrieved 18 May 2015 from: http://blog.appfigures.com/app-stores-growth-accelerates-in-2014.

Boyles, J., Smith, A. and Madden, M. (2012). Privacy and Data Management on Mobile Devices. *Pew Internet*, [online] pp.1-19. Retrieved 8 June 2015 from: http://www.privacylives.com/wp-content/uploads/2012/09/PIP_MobilePrivacyManagement-092012.pdf .

Curtis, S. (2015). Quarter of the world will be using smartphones in 2016. *Telegraph*. [online] Retrieved 25 April 2015 from: http://www.telegraph.co.uk/technology/mobile-phones/11287659/Quarter-of-the-world-will-be-using-smartphones-in-2016.html.

Deasy, D. (2013). *TRUSTe Study Reveals Smartphone Users More Concerned About Mobile Privacy Than Brand or Screen Size - TRUSTe Blog*. [online] TRUSTe Blog. Retrieved 24 May 2015 from: http://www.truste.com/blog/2013/09/05/truste-study-reveals-smartphone-users-more-concerned-about-mobile-privacy-than-brand-or-screen-size/.

Fontana, A., & Frey, J. (2000). Interviewing. *The Art of Science,* 361-376

Gilbert, P., Chun, B. G., Cox, L., & Jung, J. (2011). *Automating privacy testing of smartphone applications*. Technical Report CS-2011-02, Duke University.

Gilles, D. P. (2014). Categories. *In Apps: All You Need To Know*. Google Play.

Gralla, P., Sacco, A. and Faas, R. (2014). *Smartphone apps: Is your privacy protected?*. [online] Computerworld. Retrieved 24 May 2015 from: http://www.computerworld.com/article/2509878/data-privacy/smartphone-apps--is-your-privacy-protected-.html.

Jorgensen, Z., Chen, J., Gates, C., Li, N., Proctor, R. and Yu, T. (2015). Dimensions of Risk in Mobile Applications: A User Study. *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, pp.49-60.

Khalaf, S. (2015). *Health and Fitness Apps Finally Take Off, Fueled by Fitness Fanatics*. [online] Flurry Insights Blog. Retrieved 2 May 2015 from: http://flurrymobile.tumblr.com/post/115192181465/health-and-fitness-apps-finally-take-off-fueled.

Miles, M. and Huberman, A. (1994). *Qualitative data analysis an expanded sourcebook*. Thousand Oaks: SAGE.

Moor, J. (1997). Towards a theory of privacy in the information age. *SIGCAS Comput. Soc.*, 27(3), pp.27-32.

Njie, C. M. L. (2013). Technical analysis of the data practices and privacy risks of 43 popular mobile health and fitness applications. *Privacy Rights Clearinghouse*.

Pappas, S. (2014). *Best Fitness Apps for 2015*. [online] LiveScience.com. Retrieved 16 May 2015 from: http://www.livescience.com/49241-best-fitness-apps.html.

Privacy Rights Clearinghouse (2013). Mobile health and fitness apps: What are the privacy risks. Retrieved 2 June 2015 fromL *https://www. privacyrights. org/mobile-Privacy Rights Clearinghousehealth-and-fitness-apps-what-are-privacy-risks*>.

Rosch, F. (2014). *Study Finds Mobile Privacy Concerns Often Traded for Free Apps | Norton Community*. [online] Community.norton.com. Retrieved 24 May 2015 from: http://community.norton.com/en/blogs/norton-protection-blog/study-finds-mobile-privacy-concerns-often-traded-free-apps.

Schneier, B. (2006). *Tracking People by their Sneakers*. [online] schneier.com. Retrieved 22 May 2015 from: http:/https://www.schneier.com/blog/archives/2006/12/tracking_people.html.

Sunyaev, A., Dehling, T., Taylor, P. and Mandl, K. (2014). Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association*.

Warren, S. and Brandeis, L. (1890). *The right to privacy*. Quid Pro.

Wetherall, D., Choffnes, D., Greenstein, B., Han, S., Hornyack, P., Jung, J., ... & Wang, X. (2011, May). Privacy revelations for web and mobile apps. In *Proc 13th USENIX Conference on Hot Topics in Operating Systems* (p. 21).

Yildrim, E. (2012, May). *Mobile Privacy: Is There an App For That?* University of Amsterdam. Retrieved from http:/http://www.internetscriptieprijs.nl/downloads/scriptie_yildirim.pdf

Yoganathan, D., & Kajanan, S. (2013). Persuasive Technology for Smartphone Fitness Apps. In *PACIS* (p. 185).