www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 9 September 2017, Page No. 22486-22497
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i9.16

User Awareness of Privacy Concerns Posed by the Use of mHealth Apps

J.I. Apuru[1], D.R. Andembubtob [2], A.K Dodo[3]

[1]Taraba State Unversity, Faculty of Science,
Department of Mathematical Sciences
[2]Taraba State Unversity, Faculty of Science,
Department of Mathematical Sciences
[3]Taraba State Unversity, Faculty of Science,
Department of Mathematical Sciences

Abstract:

The proliferation of mobile devices such as phones, iPads, tablets, PDAs and other handheld devices, in the society have revolutionised how human activities are carried out today. Jobs and tasks which were erstwhile undertaken only by professionals and specialised institutions within a certain confined environment are now done by individuals who are novices by the mere advantage of owning a mobile device. The health industry is one of the sectors reaping the benefits of this advancement and large number of mobile devices with the applications used on them, mainly Mobile Health Applications. It is observed that this knowledge poses privacy concerns among users of these apps on their mobile devices. Therefore, we propose a research to assess user's awareness of their data privacy as it concerns the requesting, collection and usage of their personal information by mHealth applications. We focus on how, when and why these personal data are collected from users in the use of mHealth applications. From our study, it is observed that users, who show indifference concerning their data privacy, have come to know that they can't install mobile apps without granting certain permissions. Users' nonchalant attitude towards how their personal data are collected and used online is seen in the fact that they say nothing in the User Review section to complain. Also in an online survey conducted most of participant say they review required permissions and apps privacy policies; and read other users' review but still installed the apps since they needed to use them. This also affects the adoption of responsible practices by developers. It is argued that had developers seen users showing serious concern over their data privacy they would be more responsible in handling these data during the development of their apps. Non-adoption of responsible research in mHealth apps development places users' personal (identity) data at a high risk of mismanagement.

Keywords: Android Ecosystem, Privacy, mHealth app, Responsible Response Innovation (RRI)

1. Introduction

The use of mobile devices, especially smart phones, continues to revolutionize human life and every sector of society seeks to benefit there from (Lane 2010). The Health sector is also actively involved in this revolution today, resulting in the use of many mobile devices and applications in health areas such as in vital signs monitoring, minor diagnosis and suggesting healthy diets (Lau et al 2013). The increase in availability of these smart devices causes a general increase in the integration of computing technologies into our professional, social and private lives. The ubiquity of computing comes with enough ethical issues and concerns that needed to be known by both computer professionals and users. We propose a research on the investigation of, and intervention with the current state of applying responsible practices in mobile applications development particularly focusing on requesting, collecting, storing and processing user personal data such as identity, location, network usage, etc. especially in the health sector. We argue that the development of mobile applications should follow the principles of *Responsible Research and Innovation* (RRI) as it deals greatly with users' personal and privacy data. Responsible Research and Innovation in mobile applications can boost user confidence in the use of mobile applications, and therefore increase their popularity.

Furthermore, mobile landscape is so large and is ever-increasing; this study is rather limited to one sector of human endeavour, the health. Our consideration of mobile apps is more concerned with Mobile Health Apps (mHealth apps). Bandyopadhyay (2014) added, that privacy concerns could be the same or similar to those of other mobile applications. Indeed, the proliferation of smart devices (such as smart phones) in our society does come with its negative effects which includes exposed user data privacy as users have to grant certain permissions to various apps to access certain data from their devices before they can install or use them. The users of mHealth apps (just like all mobile apps users) are expected to know how their personal data are being collected and how they are handled, managed and used. This will give them the confidence to more readily provide these data or information and also avail them the benefits the apps are developed to offer after all. Unfortunately, most times users of these smart devices do not even know about their personal data being accessed and collected by applications running on their own devices. The developers either do not apply best practices in seeking user permissions for collecting their personal data or else, the users are negligent on their own part (where these practices exist and are applied), not paying enough attention when installing the apps on their devices (ACM 1992).

This research aims to find out if users of mHealth apps are aware of (and if they show any concern about) their personal data being collected by the apps and the privacy issues that could arise there from. A number of *Mobile Health Applications* (mHealth apps) are analysed to identify the private data they require from users; and to classify evidence where excessive and unnecessary access to user privacy is attempted; focusing on the permissions requested by these mobile apps. We analyse patterns in terms of responsible practices of data collection by the apps and show how third-party components could also affect the resulting product (Mobile Apps); for example, *"...potential privacy and security risks [also] posed by embedded or in-app advertisement libraries"* as stated by Grace et al. (2012). We also contacted mHealth apps developers to find out if they are familiar with the concepts of RRI; whether they apply responsible practices when it comes to collecting user data, and whether any form of accreditation would motivate them to adopt the Responsible Research and Innovation toolkit. We finally present the results of our findings and recommendations on how to make mHealth apps developers improve upon responsible practices which will better protect the privacy of their users' personal data.

2. Issues in using mHealth

In recent time, mobile devices have influenced, and revolutionized every segment of human life. The increase use of these devices in our lives especially in the Health sector (to check vital signs, diagnose diseases, in keep fit exercises and suggesting healthy diets, etcetera) have also incorporated computing technologies into our professional, social and private lives. Regrettably, the presence of computing and smart devices everywhere comes with ethical issues especially concerning user data privacy as users of mobile applications (apps) have to grant certain permissions to the apps before they could install them on their smart devices. As it is for all mobile apps, users of mHealth apps need to know that their personal data are being collected and know how they would be handled, managed and/ or used. We sought to find out if the developers of mHealth Apps adopt best practices in handling user data and whether the users themselves showed any concern about the privacy of their personal data being collected by the mHealth apps.

2.1 Permissions to install mHealth Apps

Permission is a mechanism used on many platforms including Android, Facebook, and etcetera; for ensuring that mobile apps do not use user private data without the users' consent. Until the previous version of Android (5.X), the permissions were granted exclusively during installation with a once-off acceptance of them. As from the next version (6+) of the Android system, permissions can also be granted on demand when the corresponding feature is needed (e.g. ask for the user location only when the app is used to display a map). A common theme in many papers is that the permissions mechanism is overly complex and that permission requests are not often understood by users who sometimes are even uncertain of which permissions are typical for what applications; (Tchakounte 2014). Similar results were reported by Felt et al. (2012) who queried whether the Android permission system effectively warns users regarding the permissions they grant during the installation of mobile applications. The study argues that the current system where the users are expected to have control (and to some extend the responsibility) of approving permissions for apps, has not worked very well in practice. Almuhimedi et al. (2015) indicated that users of Smart phones are most times unaware of the data collected by apps running on their devices. In another study, Prasad et al. (2012) argued that if users do not control the collection and sharing of their own personal health information which are collected through mobile health (mHealth) devices and applications, they would be less willing to use these devices thereby limiting their chances to gain from them; as Liu et al. (2014) also argued that a possible solution to this would be the clustering of user privacy preferences in profiles. As suggested by their results, while people could have diverse preferences for mobile apps privacy, a comparatively small number of profiles can be identified that offer to meaningfully simplify the choices made by mobile applications users. Similarly, Frank et al. (2012) studied the permission systems of Android and Facebook apps and found that applications with low reputation are more likely to deviate from the permission request patterns than high-reputation applications, suggesting that user satisfaction or application quality could be viewed from the permission request patterns of the application.

2.2 Risks of using mHealth Apps

Grace et al. (2012) focused on potential privacy risks that are posed by embedded/ in-app advertisement libraries (or ad libraries). They stated how in recent times the sale of smart phones has increased explosively, which has brought about the availability of several mobile applications to which many consumers and end-users are severally attracted due largely to the features they offer. The application developers are able to benefit from the apps both directly (when they sell the apps to users) and indirectly by embedding advertisement libraries in the applications. In most cases, developers of these apps embed the ad libraries for their own benefit but the users are unaware how they work; that is, if they even know they exist. With the increase in the capabilities of mobile devices, monitoring one's personal health isn't that difficult anymore. Different devices such as wrist watches, bracelets and other hand held or wearable devices are used to monitor one's temperature, blood pressure, calorie level and so on. But again, these devices carry on them applications that tend to interact with user information, posing privacy and security risks sometimes. Besides, there also exists the risk of users applying wrong usage of the applications thereby resulting in wrong diagnosis and/ or prescriptions and hence, causing more damages than cure. Huuskonen et al. (2015) decried the risks posed by these apps on privacy, risk also of mismanagement or mishandling of data, misinterpretation or misapplication of information and sometimes incorrect health diagnosis leading to wrong treatments and hence posing danger to the user. The Google Android market is said to have had over ten (10) billion downloads of apps recently. The ease with which applications are now developed and shared, coupled with this wide user base could attract fake and malicious applications developers and at the same time cost users' their money and violation of their data privacy; Sarma (2012).

2.3 Advantages of using mHealth Apps

According to Huuskonen et al. (2015), personal health monitoring is now a hot topic. Just using gadgets like the bracelets and other devices, one could monitor one's heart rate, schedule periods for exercising, sleep, and so on. Users are serving as doctors and coaches for themselves today due to the availability of these smart devices. This leads to better living conditions for citizens; which in turn helps the society to reduce unnecessary spending on healthcare and also helps in guaranteeing healthier citizens. Huuskonen et al. (2015) also believe that the importance of Health Data goes beyond just healthcare. For example, insurance companies and advertising outfits could also make use of user health information to plan the running of their organizations.

2.4 Health Rating Sites, mHealth Apps and User Reviews

Producers of goods and services who intend to improve upon the current stage of their productions are willing to allow the consumers of such goods and/ or services make inputs through their review of the products. Similarly, developers of applications (apps) and online sites use user reviews to improve upon their developments. For users to review an app, they must provide certain personal data that the developers can use to further reach them if required. User reviews may not always be pleasant as sometimes the users express their dissatisfaction with the app or with the site. Be that as may be, both negative and positive reviews are useful to developers of mobile apps and web sites for the improvement of their developments. Today however, some developers and providers violate their users' data privacy in order to counter the users' seeming negative comments in review of their apps, products and/ or services. According to Ornstein (2016), instead of take advantage of user reviews on sites like YELP (http://www.yelp.com/)

which is an advertisement site for several products, some health providers have resulted to defending themselves and their products and in the process violating the data privacy of their users. He showed how arguments spilling out openly on this rating site have caused professionals like doctors, massage therapists, dentists, chiropractors, etcetera, to disclose patients' medical details in a manner that is not in keeping with responsible practices. Their actions are not in keeping with best practices concerning user personal data privacy. Ornstein (2016) opines that Health professionals are becoming more familiar with the veracity of consumers rating them on sites like Yelp, both positively and otherwise. Although most user reviews could be positive, in responding to the few negative ones, some of the providers seem to violate the federal patient privacy law known as *Health Insurance Portability and Accountability Act* (HIPAA) which prohibits them from revealing any patient's health information without the patients' consent. Also according to Ornstein (2016), a research carried out on Yelp identified over three thousand, five hundred (3,500) lowest (one-star) reviews where patients mention privacy or HIPAA. In a number of instances, complaints about medical care got responses that resulted in disputes over patient privacy where the affected patients claimed dual effect of poor medical services and private data violation. Where users of sites or apps feel that their data privacy is not guaranteed, they may be forced to back off from the use of such systems and hence not be able to benefit from the service the system was meant to offer. Ornstein (2016) also mentioned the case of a client of a dentist in California who had written in 2013 how he posted a negative review on Yelp about his dentist's services; alleging that the dentist thereafter posted a response with details that included his personal dental information. This prompted him to remove his review from the site to protect his medical privacy. He further reported this to the Office for Civil Rights within the United States Department of Health and Human Services, which is responsible for enforcing Health Insurance Portability and Accountability Act. The dentist was warned by the office against posting user personal data in response to reviews on Yelp. According to the office's deputy director of health information privacy, when health professionals respond to user reviews online, they could speak generally about the way their patients are treated; but must not discuss individual cases unless they have permission to do so. Patients rating their health provider publicly shouldn't be used by the health providers as enough reason for them to rate the users back or to display their medical information without their consent. Providers of medical and health services are expected to take user reviews in good faith and not treat them on individual basis. More needs to be done by medical and healthcare providers therefore, considering that some of them still violate the Health Insurance Portability and Accountability Act which prohibits the disclosure of any patient's health data without permission and no matter for what reason(s). Most times, the patients who showed concern about being injured by health systems first complain of possible poor services they received and then the disclosure of their private data. Knowing of exposure of their privacy could effectively dissuade users (patients) from using the system and for these, clients of dentists, chiropractors and other healthcare practitioners are said to remove their comments from review sections when they see that details of their medical information are being placed online because of the reviews. They do this so as to protect their medical data privacy. Both the U.S. "Department of Health" and "Human Services" which enforce the Health Insurance Portability and Accountability Act warn against posting personal data in response to system reviews. As patients discuss the conflicts they have over reviewing systems online, they are said to have turned to rating sites with the hopes that they could help others who desired help as they share their experiences online. However, the responses they get from their service providers cause them to lose some trust in the health providers.

Also, according to Ornstein (2016), Deven McGraw, the deputy director of Health Information Privacy in the Office for Civil Rights within the United States Department of Health and Human Services is said to have called on health professionals to be more general when they respond to online reviews about how their patients are treated and only speak on individual cases when they have permission to do so; and that the practitioners do not have the right to publicly display patients' medical data just because of their comments and reviews rating their health services low. He also mentioned Jeffrey Segal, who is said to be a former critic of review sites, who is known now to encourage the positive use of these reviews by doctors.

Overall, user reviews and comments are actually meant to help experts know how well their services or systems are able to meet user needs, and to enable them get feedbacks to improve their systems. So, user comments shouldn’t be used by health providers as a kind of tool for retaliation. Just because patients (or users) have poorly rated them or their services doesn’t give the health providers the right to violate the users' privacy in return. Health providers can respond kindly and politely to their users no matter how the patients have rated their services. For example, particularly if the patient’s complaint is on unsatisfactory services, the practitioner could simply say “we’re doing our best to improve on this service” and calmly apologize. Like advised by Deven McGraw, health providers should not take user comments as personal but respond to them on general terms and politely.

The ageing population of the world places a high demand on the healthcare subsector for technology advancements. All stakeholders in the health subsector (including health industries, healthcare providers and patients) could benefit from products of technology innovations. However, developing these technologies is costly and time-consuming; and also poses challenge to ethical and privacy concerns of the users of the technology. This research is necessary therefore to identify what could be done to make mHealth apps developers adopt practices that enhance users’ data protection and encourage the use of technologies in healthcare which will as a result improve the quality of life of the user and the society, making healthcare more readily accessible and more effective. As a result of the increased demand for these apps, many developers are out in the field designing and developing different and various applications of varying capacities and usefulness. Because of the high rush to application development occasioned by high demand of these mHealth apps, not all applications developed for the healthcare subsector would be beneficial to the stakeholders in the same way. Some may be more useful than others while some may even be of little or no benefit at all to the users. While some of these health apps benefit patients to better their healthcare quality, the healthcare workers/ practitioners are benefited in the area of ease of work as benefits of cost-effectiveness can accrue to insurance companies and so on. Developers of mHealth apps need to be encouraged to observe responsible research and innovation. Otherwise, users of the mHealth apps would be in danger of their data privacy being infringed upon.

3. Method and materials

Users of mHealth apps (just like all other apps) are required to grant certain permissions to the developers via the Mobile Apps store before the apps can be downloaded and installed on their mobile devices. In the latest versions of Android you can also forgo the process of approving permissions during installation, and instead approve (or deny) access on demand during runtime. The permissions given by users provide the apps with access to specific capabilities or information on their devices, such as position, address book, etc. For example, users are shown which data an app would access from their devices when they preview such an app on Google Play. This information is intended to help users decide whether to install the app or not, depending on how reasonable the required permissions are to them. The most important permission groups normally appear on every download screen while the full list of permissions for an app may be found by following a link (usually provided by the developers).

We study the permissions users are required to grant before they could download and install mHealth apps on their mobile devices (with particular interest in personal data collection handling by developers). We also contacted developers and users of mHealth apps (via online questionnaires) to survey their level of applying responsible practice and showing concern on their personal data privacy respectively.

3.1 Data Collection

We collected thirty-five (35) mHealth apps from the Android Ecosystem and studied the permission requests by the apps to identify where an app attempts to make excessive and unnecessary access to user personal data. There are several mobile apps on the Google Play Store from where we identified the health related apps for the study. Different types of mHealth apps exist ranging from those used for fitness exercises to those used for health records and for diagnostic purposes. We collected information from user reviews on the 35 apps selected and their privacy policies from their respective web pages; and also contacted the developers to assess their level of awareness and adoption of Responsible Research and Innovation (RRI) in collecting and using user personal data when developing their apps. A Java program was written and used to crawl the apps sites for user reviews from where we try to check for user comments showing concern over their personal data. The Program uses the uniform resource locators (URLs) of the thirty-five (35) apps to trace all current *"User Reviews"* concerning them from the popular Google Play Store and save it to a text file. We then try to check out the comments in the reviews that suggest that the users are concerned about the privacy of their personal data. On the users review text file we use the 'Find' function, to search for key words such as 'private', 'privacy', 'concern', 'personal', 'data', 'information' and then check out the sentences where they appear. Most of the 35 apps collect data such as User Identity, Contact details, Calendar, Location (approximate and precise), Photos and Storage, Camera and Other Sensors. The analytical table of these permissions is presented in Table 1. We analyze user reviews on the apps to assess users' level of awareness of the fact that these apps collect such data from them; and how concerned they are about the privacy of their data being thus collected. There is no significant mention in the reviews by users of the apps to show that they are aware of, or that they are concerned about the privacy of their personal data being collected by mobile apps. This could be a result of one or more of the following possibilities:

1. The developers do not make the collection of user personal data explicit enough for the users to see and show concern about the privacy thereof.
2. The users do not pay enough attention to notice that their personal data are being collected when they download and install these apps on their smart phones.
3. Some users might have read up the Privacy Policies regarding the collection, management and use of the personal data collected by the apps and is comfortable with it.
4. Users are aware of the fact that they cannot use the apps if they do not provide these data or grant the permissions for the apps to access them and so, they give in to good faith and release the information. This is especially true when they know that the apps are meant to be helpful for them.

3.2 Data Analysis

To find out if developers of mHealth apps apply responsible practice when developing their apps, we collected data from the apps privacy policy page where this is available. This helps to identify what type of data each app collects from its users and what privacy policies the app developers adopt to let the users know what is at stake (if any) when they place their personal data online to download and install the apps. We also examined the manner in which the developers relate with the users to access these data. In the first case, we try to know if the apps require permissions to collect such data as Identity, Contact, Calendar, Location, Photos and Storage, and Camera. In the second instance we try to find out whether these mHealth apps developers explicitly ask for user consent to collect user data and if they specify what type of information they collect from the users; whether they explain how they maintain privacy and security of user personal data and if there are clear mechanisms to unsubscribe and delete user personal data from their servers when required. We also try to find out if developers explicitly say whether they will sell and/ or share user data with third-parties; and if they have clearly spelt out Privacy Policies which users may use to understand how their data is protected. A detailed investigation leading to collection of data herein is included in Appendix 1. We also attempt to find out directly from the developers (via online questionnaires) whether they are familiar with, and apply responsible practice; and whether any form of incentives will make them more willing to adopt responsible practice. We sent out online questionnaires to the thirty-five (35) developers whose apps we study. Unfortunately we only had responses from three (3). Results of the questionnaires also provided data for the question as to what would motivate developers to more readily adopt responsible practices.

In order to find out users' level of awareness of their personal data being collected when they install mobile apps and the privacy concerns thereof, we crawled user reviews for the apps using a Java program, to see if they express concern over the privacy of their data. Unfortunately, this did not give much result. We therefore contact users of mobile applications online. We sent questionnaires to 132 users and had responses from 39. The questions and results for the online survey are presented in the Results and Appendices sections respectively.

3.3 Offline Analysis of App Permission Needs

Of the 35 apps selected, we reviewed the types of data the apps require permission to access from the users. The results are summarized in Table 1:

Table 1: Data Types required by mHealth Apps

S/ N	Data Type	Require d	Not Require	% Required

			d	
1	Identity	24	11	68.57
2	Contacts	23	12	65.71
3	Calendar	3	32	8.57
4	Location	19	16	54.29
5	Photos and Storage	31	4	88.57
6	Camera	22	13	62.86

Only three (3) out of thirty-five (35) apps analyzed (a very small percentage of 8.57%) require permission to access users' calendar while thirty-one (31) out of thirty-five (35) apps, representing a very high percentage (88.57%), require user permission to access user Photos and Storage. Twenty four (24) apps (68.57%) require permission to access user identity data. These are the data that identify the users and hence, their personal data. 23, 19 and 22 apps representing 65.71%, 54.29% and 62.86% require permission to access Contacts, Location and Camera respectively from the users' devices.

We study to further understand if users' personal data; including their identity, photos, locations (sometimes, even precise location) are so much required by the apps, do the developers do much on their own part to let the users know their apps would collect such information from them. Here, we ask questions about developers' mode of collecting the information from users and whether they show in any way how this information will be treated. The results are presented in Table 2.

Table 2: Responsible Practices by Apps Developer

Answers to Responsible Practice questions	**Ye s**	**No**	**% Yes**	**% No**
Do developers explicitly ask for user consent to collect User Data?	15	20	42.76	57.1 4
Do developers specify what type of information they collect from users?	30	5	85.71	14.2 9
Do developers explain how they maintain Privacy and security of user personal data?	14	21	40.00	60.0 0
Is there a clear mechanism to unsubscribe; and delete user personal data from their servers?	8	27	22.86	77.1 4
Do developers explicitly say whether they will sell/ share user data with third-parties	14	21	40.00	60.0 0

For twenty (20) of the thirty-five (35) apps reviewed, which is some 57%, their developers do not explicitly seek user consent to collect their personal data. The area where one could infer that developers collect data from users is mostly in the places where a whopping 85.71% require the users to grant permissions for the apps to access certain information before they are able to install them. Unfortunately, most times such language is not clearly understood by the users to mean that their personal data would be collected and stored away from their handheld smart phones. Developers of twenty-one (21) of the thirty-five (35) apps, being sixty percent (60%)do not say clearly how they maintain the Privacy and Security of User Personal Data; and another 60% do not clearly say whether they would sell/ share User Personal Data with third parties. For twenty-seven (27) apps of the thirty-five (35) which is 77.14%, users are not even given any chance to know if and how they may wish to unsubscribe and delete their Personal Data from the Servers where they have been collected and stored some far away from their mobile phones. About 54% of the developers of the mHealth apps under consideration put up some kind of Privacy Policies that give users the opportunity to read through and know everything surrounding the privacy of their data collected by the apps. Users however, do not always have the patience to read through these policy statements as most times they are not so precise and straight to the point.

3.4 Feedback from mobile app users (via online questionnaires)

The online survey on user perception of data privacy got responses from thirty-nine (39) respondents which included both male and females and cut across different age groups as shown in Figures 1 and 2.

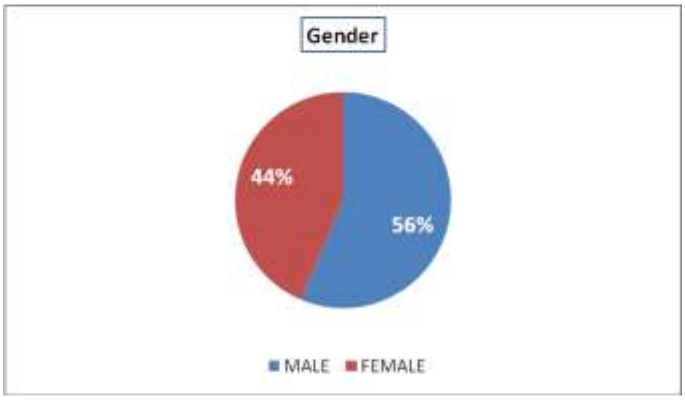

Figure 1: Respondents' Gender

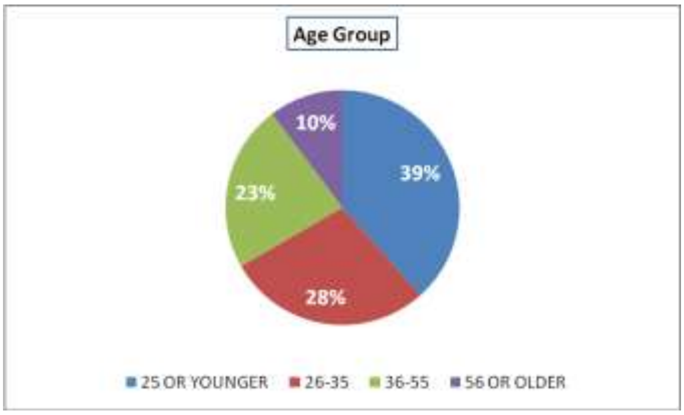

Figure 2: Respondents' Age Group

Forty-six percent (46%) of the respondents said they have one time or the other installed health related apps on their mobile devices, forty-nine (49%) said they haven't installed any health apps while five percent (5%) are unsure. It didn't make so much difference though, as privacy could be viewed as serious in all age groups.

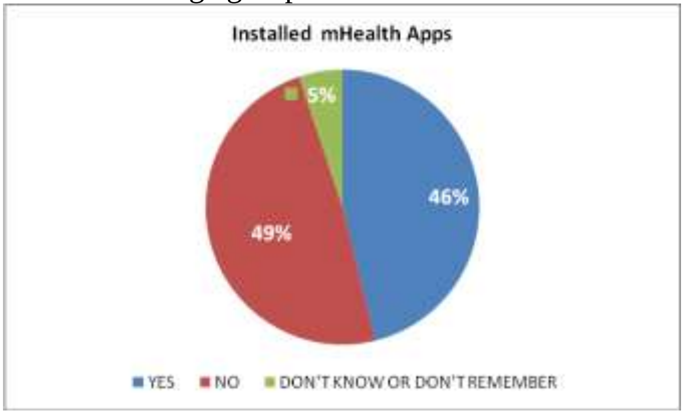

Figure 3: Respondents Who Installed mHealth Apps

Do users review the permissions they grant when they install apps on their smart phones? The results presented in Figure 7 suggest that most users do. Only about eighteen percent (18%) are either ignorant of the permissions or do not see them as important. 82% of our respondents take their time to review the permissions required by the apps.

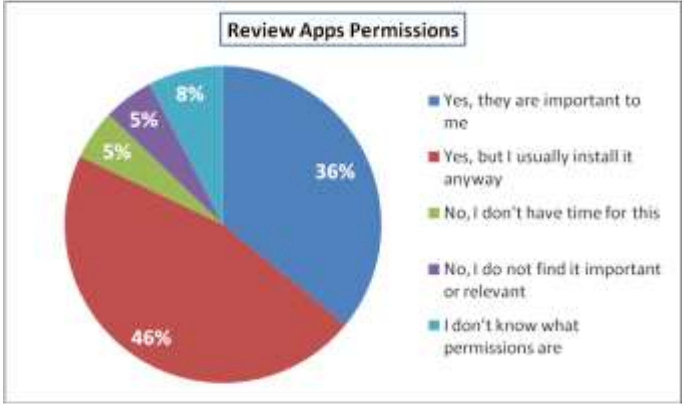

Figure 4: Respondents Who Review Apps Permissions

Most users also take time to review apps' Privacy Policies and to read other users' review relating to how developers handle users private data before installing them on their devices. This can be seen in Figures 5 and 6 below:

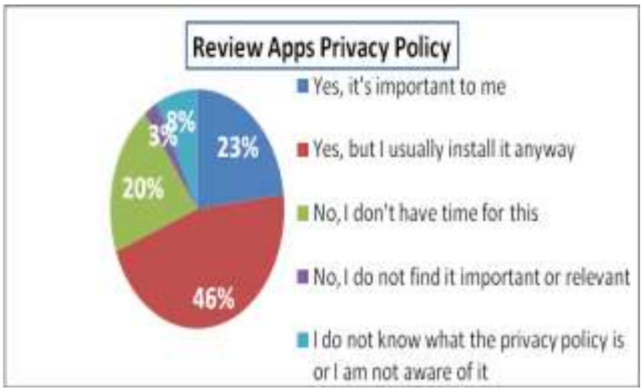

Figure 5: Respondents Who Review Apps Privacy Policies

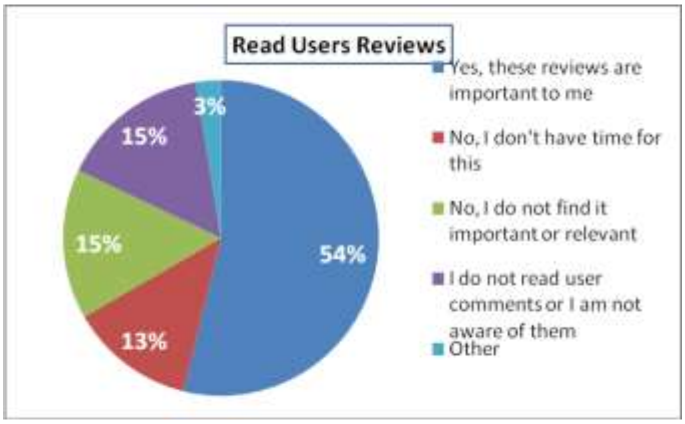

Figure 6: Respondent Who Read User Reviews

4. Discussion and Critical Evaluation

This study proposes that most of the Permissions required by the apps are not necessary for the purposes for which the apps are developed. For example, it does not make a lot of sense why an app which is developed to help users lose weight and monitor their blood pressure (such as *Health Mate*) would want to have access to the users' contacts. Since the contact details on the users' device wouldn't be used in tracking users' weight or monitoring their blood pressure, it can only be assumed that the developers will collect this data not for explicit use for the intended purpose for which the users are granting the permissions. Another case is that of an app, "*Drugs Dictionary"* which is a useful and friendly drugs dictionary and provides information about drugs: uses, dosage, side effects, precautions, drug interactions, and missed doses. Being that this app is just a drugs dictionary; its request for so much data from the users is rather questionable (e.g. it requires permission to collect user data including identity, contact details and both approximate and precise location. Data such as precise location and users' contact details do not appear to be relevant for such an app as a drugs dictionary which is just to be used by users to gather information about drugs, their dosage and side effects. We opine here that most developers collect some of these personal data from users' devices for uses other than the users would be willing, most likely for use with third-parties. This is in consonance with the opinion expressed by Grace et al. (2012). To answer the research question as to whether developers of mHealth Apps apply Responsible Practices while developing their apps, it is observed that most of the developers do not apply responsible practices. Most developers are not even aware of what responsible practices are and so cannot possibly be expected to apply the RRI kit.

Whether users are aware of the permissions they grant and if they show any concern about the risk of placing their personal data online is another question this study seeks to address. We find that most times users are not aware of the data which mobile apps are able to access from them when they grant permissions to install the apps. This position agrees with, and is a common theme in several opinions in the literature which expresses that the permission mechanism is rather complex and users don't usually understand the permissions they grant (Felt et al., 2012;Tchakounte, 2014; Almuhimedi et al., 2015).Although users do not show much concern in the user review sections during apps installation, in our online survey they claim knowledge of the permissions they grant when they install apps. Most users are also concerned about the privacy and security of their data. Unfortunately they say to have granted these permissions since they couldn't install the apps without allowing access to the required data. Also, it is found that developers would more readily adopt responsible practices in their developments of mobile apps if there were a form of incentives.

Also, in trying to find out how well the developers handle their request for permissions to access user data we found that majority of developers of apps analysed in this study (20 of 35 which is about 57.14%) do not explicitly ask to collect data from the users even though they do. The areas where most developers suggest that they collect data from users and specify the type of data (a whopping 85.71%) is in the places where they require the users to grant permissions for the apps to access such information before they are able to install them. Unfortunately, most times such language used in seeking these permissions is not clearly understood by the users to mean that their personal data would be collected and stored away from their handheld smart phones. About 60% of the mHealth apps developers do not show clearly how they maintain the privacy of user data and another 60% do not clearly state whether they would sell or share user data with third-parties. Less than 23% of the developers of the mHealth apps studied show clear mechanisms to unsubscribe and delete user personal data from their servers if the users so decide. Hence for the greater percentage of the apps, if the users decide not to use the apps again someday, their data continue to reside on the developers' database which is not supposed to be, especially without the consent of the users. The users are supposed to be the final point of control to their own personal data and decide whether or not they wish to delete their data from the developers' database whenever they wish to discontinue the use of any apps. There are a few cases where the developers show that they maintain the highest sense of Responsible Practice in their development via the way they handle user data. In one of such cases, developers of the app *Symptomate Symptom Checker* collect no personal user data for storage on their database. The app is an innovative symptom checker designed by doctors to help users find out more about symptoms of a wide range of ailments. It is said to have provided well over 500,000 health check-ups. Users enter basic information about their health complaints and receive a list of potential diagnoses and a recommendation of doctors they could contact. The app asks users a few carefully selected follow-up questions regarding their symptoms. It is driven by advanced artificial intelligence algorithm which uses a broad medical database of over 1000 symptoms and over 500 potential conditions. The medical database of symptoms is carefully created and curated by a team of experienced physicians. Another app that does not collect user data for storage in its database is the *Health and Nutrition Guide*. This app contains huge collection of Health Tips, Nutrition Tips, Nutrition Calculators, Home Remedies and Health Recipes which help users to maintain and improve their health and fitness. Only these 2 from amongst the 35 apps here analyzed (barely 5.71%) do not collect user data to store in their databases. Two other apps which also do not collect user data so vigorously but seeking permission only for access to user camera are *Heart Rate Monitor* and *Heart service*. The dual are used for measuring user heart rate. Heart Rate Monitor is a cardiograph for user's Android device, giving results to enable users check their heart rates on real time basis. The app measures user's heart rate by analyzing blood flow on the tip of his/ her finger. Similarly, the Heart service app uses medically correct methods to measure users' heart rate and heart rate variability using the camera of user's smart phone. For these two, it is understandable why the apps should need access to user camera. Four (4) apps (representing 11.43%) each collect at least a couple of the user data queried in this study but they also explicitly seek the users' consent and explain how they maintain user data privacy and if they share user data with third parties for any reason.

We see from this study that often mHealth app developers do not strictly observe responsibility practices in developing mHealth apps. This lack of adoption of Responsible Practice could be caused by different reasons including ignorance of *Responsible Research and Innovation* (RRI) on the side of some developers while others could be due to lack of incentives.

4.1 Users' Nonchalant Attitude towards Data Privacy

One other reason that could negatively affect developers imbibing responsible practice is users' nonchalant attitude towards their own data privacy. This study reveals how a great percentage of the users of mobile apps review required permissions and apps privacy policies; and also read other users' review relating to how developers handle data privacy and still go ahead to grant permissions and install apps without expressing any concern in their own reviews. These could be seen in Figures 4 to 6. So, if the users whose data privacy could be at risk do not show any form of concern, the developers may also careless about the data privacy. If users express enough concern online and show skepticism about the several personal data for which they have to grant access to apps, fewer users would like to install such apps and that would encourage the developers to treat user data more responsibly.

6. Conclusion

We show that awareness of responsible practices amongst mHealth apps users remains low. When users are not aware of responsible practices in collecting or managing their personal data then they stand the risk of forfeiting the privacy of their data and the security thereof. We agree with Huuskonenet al. (2015) who decried the risks posed by these apps both on privacy and(sometimes) in mismanagement or mishandling of data, misinterpretation or misapplication of information. These could lead to incorrect health diagnosis and wrong treatments which can be quite dangerous to the users. On the other hand, we believe that if mHealth apps are developed responsibly and used appropriately, they would be of much benefit to the users and help them to live quite healthily. Huuskonen et al. (2015) also believes that the importance of Health Data goes beyond just healthcare and reaching forth to areas of human life such as insurance, etc. The present level of applying responsible practices by mHealth apps is inadequate and needs to be improved upon and doing this requires conscious efforts, both from developers and users of mobile applications as well as from governing authorities like the Government and Computing Professional Societies. The governing bodies should consider giving incentives to mobile applications developers who apply responsible practices while penalizing defaulters. On their part, users need to take the privacy of their own personal data more seriously. They need to express more concern over their data privacy especially when they review apps online. Finally, the developers should be more professional and handle users' personal data more responsibly, knowing that users reveal these data details to them on trust. Developers need to know that if users discover that their personal data is not handled in accordance with best practices and the privacy and security thereof maintained, they would likely opt out of the use of the apps. This agrees with the theme expressed in Ornstein (2016).

Personal information privacy is important and so developers, users and third-parties should both work towards the safety of user personal information as much as possible, employing best/ responsible practices. Developers especially, should apply responsible practices when the collect, store, manage and use users' personal data. Low level of adoption of responsible practices by developers of mHealth apps is seen in the fact that most of them do not do enough to inform their users of the data they collect from them, how these data would be stored, used and how they secure them. Users are not usually shown how they may opt out from sharing their data and deleting them from developers' databases. In most cases, when developers include privacy policies requesting users to grant permissions before installing their apps, the language used is not explicitly clear to allow the users know that there was anything at stake. Unfortunately, in very few instances where the developers try to apply responsible practices, most users are somewhat careless about their personal data, not taking time to carefully read through the apps Privacy Policies and consider before granting permissions to install the apps. Developers need to be more explicit when asking for permission to access users' personal data and to show how the users may delete their data from the developers' databases if required. The study reveals that most developers do not adopt responsible practice in mHealth apps development due to ignorance of *responsible research and innovation*; while some would adopt responsible practice if there was some kind of *incentives* for applying responsible practices or if there was some kind of *penalty* against lack of adopting responsible practices in mHealth apps development. Another reason for developers' carelessness about responsible practices is that users also do not show enough concern about the security of their private data. Users need to be encouraged to show their concern online in the User Reviews section. This helps keep the developers on their toes in adopting responsible practices. Prasad et al. (2012) argued that if users do not control the collection and sharing of their own personal health information which are collected through mobile health (mHealth) devices and applications, they would be less willing to use these devices thereby limiting their chances of enjoying from them; which will defeat the purposes for which the apps are developed.

References

1. ACM, 1992-last update, ACM Code of Ethics and Professional Conduct [Homepage of ACM], [Online]. Available: https://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct [08/10, 2016].

2. ALMUHIMEDI, H., SCHAUB, F., SADEH, N., ADJERID, I., ACQUISTI, A., GLUCK, J., CRANOR, L. and AGARWAL, Y., 2015. Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging.*CHI '15 Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, , pp. 787-796.

3. Bandyopadhyay, T., & Zadeh, B. (2014). Mobile Health Technology in the US: Current Status and Unrealized Scope. In *Social Media and Mobile Technologies for Healthcare* (pp. 304-321). IGI Global.

4. FELT, A.P., HA†, E., EGELMAN, S., HANEY†, A., CHIN, E. and WAGNER, D., 2012. Android Permissions: User Attention, Comprehension, and Behavior ,*SOUPS '12: Proceedings of the Eighth Symposium on Usable Privacy and Security*, July 2012 2012, ACM.

5. FRANK, M., DONG, B., FELT, A.P. and SONG, D., Minning Permission Request Patterns from Android and Facebook Applications.

6. GRACE, M., ZHOU, W., JIANG, X. and SADEGHI, A., 2012. Unsafe Exposure Analysis of Mobile In-App Advertisements *WISEC '12: Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*, April 2012 2012, pp. 101-102-112.

7. HUUSKONEN, P., HÄKKILÄ, J. and CHEVER, K.T., 2015. Who Needs a Doctor Anymore? Risks and Promise of Mobile Health Apps, *MobileHCI '15: Proceedings of the 17th International*

Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct, August 2015 2015, ACM, pp. 870.

8. LANE, N. D., MILUZZO, E., LU, H., PEEBLES, D., CHOUDHURY, T., & CAMPBELL, A. T. (2010). A survey of mobile phone sensing. *IEEE Communications magazine*, *48*(9)

9. LIU, B., LIN, J. and SADEH, N., 2014. Reconciling Mobile App Privacy and Usability on Smartphones: Could User Privacy Profiles Help? , *April 2014 WWW '14: Proceedings of the 23rd international conference on World wide web*, April 2014 2014, ACM, pp. 201.

10. ORNSTEIN, C., 2016. Pro Publica. Doctors fire back at bad Yelp reviews — and reveal patients' information [online]. Available at:

11. <https://www.washingtonpost.com/news/to-your-health/wp/2016/05/27/docs-fire-back-at-bad-yelp-reviews-and-reveal-patients-information-online/> [Accessed 18/07/2016]

12. PRASAD, A., SORBER, J., STABLEIN, T., ANTHONY, D. and KOTZ, D., 2012.Understanding Sharing Preferences and Behavior for mHealth Devices, *WPES '12: Proceedings of the 2012 ACM workshop on Privacy in the electronic society* , October 2012 2012, ACM, pp. 117.

13. SARMA, B.P., LI, N., GATES, C., POTHARAJU, R., NITA-ROTARU, C. and MOLLOY, I., 2012. Android Permissions: A Perspective Combining Risks and Benefits.

14. TCHAKOUNTE,F.,2014.Research Gate.Permission-based Malware Detection Mechanisms on Android: Analysis and Perspectives [Online]. Available at:

15. <https://www.researchgate.net/publication/271199472_Permission-based_Malware_Detection_Mechanisms_on_Android_Analysis_and_Perspectives> [Accessed 27/07/2016]