A Realisation of Ethical Concerns with Smartphone Personal Health Monitoring Apps

Conference Paper *in* ACM SIGCAS Computers and Society · September 2015

DOI: 10.1145/2874239.2874285

Tilimbe Jiya
De Montfort University

A REALISATION OF ETHICAL CONCERNS WITH SMARTPHONE PERSONAL HEALTH MONITORING APPS

Tilimbe Jiya
Centre for Computing and Social Responsibility
De Montfort University,
The Gateway, Leicester
LE1 9BH
Telephone number, incl. +44 01162507475
Email:tilimbe.jiya@email.dmu.ac.uk

ABSTRACT

The pervasiveness of smartphones has facilitated a new way in which owners of devices can monitor their health using applications (apps) that are installed on their smartphones. Smartphone personal health monitoring (SPHM) collects and stores health related data of the user either locally or in a third party storing mechanism. They are also capable of giving feedback to the user of the app in response to conditions are provided to the app therefore empowering the user to actively make decisions to adjust their lifestyle.

Regardless of the benefits that this new innovative technology offers to its users, there are some ethical concerns to the user of SPHM apps. These ethical concerns are in some way connected to the features of SPHM apps. From a literature survey, this paper attempts to recognize ethical issues with personal health monitoring apps on smartphones, viewed in light of general ethics of ubiquitous computing. The paper argues that there are ethical concerns with the use of SPHM apps regardless of the benefits that the technology offers to users due to SPHM apps' ubiquity leaving them open to known and emerging ethical concerns. The paper then propose a need further empirical research to validate the claim.

Keywords

Ethical concerns, smartphone apps, personal health monitoring

1. INTRODUCTION

As smartphone health monitoring applications (SPHM apps) move from an introductory stage through societal permeation to a stage where they are widely used called the power stage [17] there are ethical concerns that needs to be made aware to users and potential users of these apps. Due to the features of SPHM apps, it is inevitable that ethical concerns will arise and that users and ethicists are aware of these. The knowledge or realisation of these ethical concerns is very important not just to the user of SPHM apps but to the developers of such technology and other stakeholders. One of the reasons for its importance is that it promotes responsible innovation through a feedback mechanism that virtually exist between the app users and developers on how to address them, either in existing or future products.

Thus said, this paper will attempt to answer the question on what are the ethical concerns with personal health monitoring apps on smartphones, viewed in light of general ethics of ubiquitous computing. Some doubt the relevance of ethics in computing technology [20] however, this paper argues that it is reasonable to suppose that the growing ubiquitous nature of SPHM apps necessitates reflection of related ethical concerns in society and calls for a stronger awareness of computer ethics in society.

The realisation of these ethical concerns could come about in two ways; firstly by looking at ethical concerns which are coherent with the features of SPHM apps for example its ubiquity and then possibly identifying generic ethical concerns [5] that are likely to be relevant to SPHM apps or secondly we could be more speculative and forecast about potential ethical concerns. This paper will however adopt the first approach, that of identifying generic ethical concerns in light of the ubiquity of the apps. In doing so, the paper conducts a literature survey on generic ethical concerns with smartphone apps and similar technology that fall within the ubicomp umbrella precisely health monitoring ones.

From the generic approach insights emerge that inform some speculation and feed into a forecast of some issues that are missed within literature and could potentially arise from the use SPHM apps. These speculative ethical concerns form the foundation of the discussion on the realised ethical concerns of SPHM apps.

The paper attempts to identify ethical concerns of SPHM apps at 3 different levels of the technology in relation to specific features that are relevant to each level of the technology and then, the paper discuses some potential novel ethical concerns of using SPHM apps and propose a need for further empirical research to validate the claim.

2. METHOD

This paper surveyed peer reviewed journal articles and conference papers from three databases namely Scopus, EBSCO Host and Google Scholar focussing on ethics of ubiquitous computing with a keen interest on mobile health monitoring. The search was limited to 10 years due to the novelty of smartphones. However, there was limited literature that specifically used the term *'smartphone'* and more specifically *'smartphone app'* therefore an inference from ubicomp was adopted merely because smartphone apps are part of ubicomp.

2.1 Process

Literature sources were systematically searched within the above mentioned databases. This involved using multiple word combinations and similar words in order to come up with comprehensive search results that were pertinent to inform the paper. Such synonymous words and word combinations as 'personal health monitoring', 'ethical concerns', 'ubiquitous mobile applications', 'pervasive applications', 'smartphone health apps' etc. were used in the literature search. The search results were scrutinised to ensure that the technology discussed was closely related to smartphone health monitoring apps according to the features described in this paper.

2.2 Analysis

As part of the realisation, the paper looked at the generic ethical concerns from, the articles that were deemed relevant. In Nvivo [3] the content of the paper was analysed in order to develop an overview of the general discourse on ethical concerns that are frequently discussed within the text. Using a word tree and frequency analysis themes were extracted and built across multiple literature sources.

Text is highlighted that had a reference or appeared to make reference to an ethical issue with ubiquitous mobile computing (ubicomp) and in some cases smartphone applications. The highlighted text was coded and the coded text segments were assigned themes. From the coding process a discussion of results emerged based on the frequency of code appearance.

5 themes were developed referring to the main generic ethical concerns realised from literature.

3. RESULTS

The literature survey resulted in 87 results and using the inclusion criteria only 27 were relevant from which 16 were selected as the most apt after reading them. The inclusion criteria used in the paper was; the age of articles had to be not more than 10 years; the main focus of the papers should be related to ubiquitous mobile applications that are related to health monitoring and their outcome should potentially discuss or suggest ethical concerns or issues with technology.

From the selected papers the following generic ethical concerns were found and were categorised into 5 themes that were more recurrent and generally applicable to SPHM apps. These themes are further discussed in the sections below.

3.1.1 Data misappropriation

One of the ethical concerns with using SPHM apps was relating to data misappropriation. The concern arise from questioning the originality of the apps and clarity on where accumulated data is stored and manipulated. Data misappropriation could be defined as the unauthorized use of user's data, without their permission and consent that has potential to result into harm. This is a great responsibility concern.

SPHM apps are developed by developers who are both regulated and un-regulated. Data can potentially be stored in servers or other storage mechanisms that are prone to malicious compromise either intentionally or unintentionally which could result into harm. A particular concern seem to be the possibility that data could be sold to private corporations and exploited for profit rather than for the public good [19].

As part of personal health monitoring, SPHM apps store personal identifiable data (PID) that could be linked to personal health data (PHD). The combination of the two can be used to identify personal information of the user [18]. Relatively, SPHM apps have the ability to reason with the raw sensor data to identify higher level information, based on established medical knowledge that is embedded within the app [4] and this raw data if fallen in the wrong hands could be used for inappropriate activities that could damage or harm the owner of such data

3.1.2 Identity theft

Another concern that emerged from the literature survey is that of identity theft. This concern is somehow related to the one above merely because identity theft occurs when a user's personal information is stolen and misappropriated to impersonate them for fraudulent activities. Data collected by apps could be used, with a few parameters, to trace even anonymised data back to the data subject in light of re-identification [21] which could then be used for identity theft or identity fraud.

A combination of user's name with other metadata, such as age and location, can identify a user by triangulation [7, 19] and then the user could be impersonated by a fraudster to carry out for instance financial transactions without their knowledge. All SPHM apps especially those that are freely downloaded may share non-personal data on usage which could potentially be combined with the universal device ID or a unique ID of the downloaded SPHM app which could then enable the non-personal data be tracked back to the user therefore identifying them [1, 19]. As mentioned earlier, this is a potential ethical concern since this data has a potential to be used for other unintended activities using the users identified ID.

3.1.3 Privacy infringement

The third concern that frequently appeared in literature is that of privacy infringement. Considering that smartphones are part of ubiquitous and pervasive computing, privacy appears in literature as one of the ethical concerns of mobile apps[10, 16]. The privacy that is discussed here is the one which mostly refers to the separation of user data and personal privacy. This privacy has a direct relationship with security of user data[18], for example during transmissions data could end up in the wrong hands [2, 6]. When people download SPHM apps their privacy is put at risk due to the apps being susceptible to outside invasion thereby affecting the users' privacy. One way that this happens is through SPHM apps that encourage users to share what could be considered sensitive and private information via social media. This is common with activity tracker apps that have their own virtual forums linked to social media in the name of bringing people together for encouragement and sharing of experiences [23].

Privacy infringement in SPHM apps is a resultant of poor data security measures that are put in place within the apps or their features. Many SPHM apps have poor data security due to the way they transmit data[18]. Some SPHM apps transmits unencrypted data using unsecured networks which could be viewed by anyone who is watching or listening on the network [1, 8].

3.1.4 Uberveillance

Another concern that emerged from the literature survey was that of uberveillance. Uberveillance involves identity and location tracking that is constant and embedded in a technology artifact which is real time ad automatic [13] Activity trackers used in SPHM apps can store information about the location and places where the user has been over a certain period therefore leaving a traceable pattern that can be used for uberveillance [12]. Smartphones on which these apps are mostly installed are constantly online and location enabled and rarely do people turn the geo-location-features off when they are out and about [1], as a result they could potentially provide location data which poses a challenge for anonymity for users of SPHM apps.

3.1.5 Legal inadequacy

The last theme that emerge from the literature survey is a concern with legal inadequacy when it comes to SPHM apps. There is lack of policies that govern emerging technologies such as apps and even if policies are in place there is inadequate policing of these policies that guarantees their effective implementation [12, 22]. In addition, the mobile apps ecosystem is unregulated especially with health and fitness monitoring apps and the data that these apps collect is mostly not covered by existing regulations that protect the privacy and security of the personal health information (PHI) [1]. This lack of legal provisions such as privacy protection could have ethical consequences to users such as identity theft and sale of identifiable data by unregulated app developers.

Another point is that is of interest is the extent of legal and cultural differences over privacy and other ethical concerns with mobile health apps between global regions, for instance over what constitutes as a medical app and issues around user consent [22][21]. Depending on the resident country of the SPHM app development, both users and developers can be subjected to different laws and legal obligations. Some regions have a weak adherence to the rule of law and limited privacy protection than others therefore users are vulnerable to abuse.

4. DISCUSSION

The pervasiveness of smartphones has facilitated a new way in which owners of devices can monitor their health using applications (apps) that are installed on their smartphones. Personal health monitoring involves behaviour interventions that will promote people's health in reaction to feedback they are receiving from their body or environment [16]. The advancement of mobile technology especially smartphones and ever growing app market, has enhanced mobile personal health monitoring [4] and gave rise to ubiquitous mobile health(m-health) which formed the basis for mobile applications that monitor personal health [11, 15]. There has been an increase in the development of apps that can be used to monitor personal health regardless of platform and expertise of user [9] and these have shifted the paradigm of self-health monitoring allowing people to accurately monitor themselves with mobile technology [14].

Regardless of the benefits that this new innovative technology offers to its users, literature shows that there are some ethical concerns to the user of SPHM apps. These ethical concerns are in some way connected to the features of SPHM apps. Smartphones are accessible by society members who have either significant or limited technical knowledge which renders them susceptible to ethical consequences that can result from use of such new technology, in this case, SPHM apps that are available on the consumer market.

During the survey, this paper could not identify any literature that specifically address ethical concerns with smartphone apps, most especially those that monitor health. However, this paper managed to find a few that were indirectly related to SPHM apps in respect of its ubiquity. Therefore, this gave the paper a starting point to discuss ethical concerns with SPHM apps.

SPHM apps are built-in, free and/or pay to download from app stores and they demonstrate versatility, usability and functionality at nominal or no cost. Their features which generally includes their ability to collect and store health related data of the user either locally or in a third party storing mechanism, render them prone to ethical concerns as a result of loopholes within their functionality for example data being intercepted during transmission. Another feature common with SPHM apps is their geo-location capability which can be used to locate and identify the user. This feature mainly mostly works with the online connectivity of the SPHM app therefore facilitates the online connectivity a real time identification and tracking of the user. As established from the literature survey, this has potential ethical implications to its user. Users of smartphones need to have knowledge on how the 'location' feature works and what sort of information could be sent out merely by not disabling the feature. This calls for some technical know-how from the user which is normally not the case with the society members at large.

SPHM apps are also capable of giving feedback to the user of the app in response to conditions that are provided to the app therefore empowering the user to actively make decisions to adjust their lifestyle. This is potentially another area of concern because this could result in the user using or misusing of health signals or feedback that they are receiving from their body via the SPHM app. In such circumstances, there is a risk of the user not understanding or inappropriately understanding these signals and leaving themselves prone to risk of self-diagnosing and medicating in attempt to quickly respond to a warning or feedback that they are receiving from their SPHM app. A practical scenario could be a user buying weight loss medication outside their doctor's knowledge, say online, which could potentially result in drug misuse.

From the literature survey we can envisage ethical concerns that are related with SPHM apps from the generic themes that appear from it. Although not a lot is directly pointing at SPHM apps, the concerns discussed in the literature gives us a foundation to speculate more on ethical concerns. In an attempt to speculate on them, this paper proposes a speculative analysis of SPHM apps. This speculative analysis of SPHM apps comprises of 3 levels of the smartphone app technology as shown in Figure 1 below. The figure shows the speculative ethical concerns with SPHM based on a focus at;

i. The features of the app such as its memory capacity that paves way for ethical concerns such as data loss or privacy violation.

ii. The specific artefact and procedures that smartphone apps are involved with therefore looking at different uses and speculative ethical concerns at that level.

iii. At the specific technology i.e. SPHM apps. At this level the speculative ethical concerns are narrowed down to the specific app looking at the specific users, context and features of the app. With regards to SPHM apps, we look at the application or use that happens within certain contexts.

Table 1. A three level speculative analysis of SPHM apps

Technology level - Smartphones		
Focus is on general features of smartphones	Core features • Ubiquity • Sensing • Memory • invisibility	Ethical concerns • Data loss • Uberveillance • Privacy
Artifact Level – Smartphone apps		
Focus is on specific artifact and procedures	Different uses • Health • Navigation • Temperature	Ethical concerns • Data loss • Data security • Storage issues • Legal inadequacy • Learnability • Privacy
Application level – SPHM apps		
Focus is on specific users and use or context	Application • Mobile health monitoring • Home use • General public • Available on consumer market	Ethical concerns • Misleading health data • Misuses of drugs • confusion

The first level is the more generic one that looks at smartphone apps and / or ubicomp and then identifies the ethical concerns. This focuses on the technology at large looking at the features that make up the technology i.e. smartphone technology.

The second one is the artifact level where the useful combination of smartphone and other novel technology procedures provides a service or new product. In this case, the consideration is on the combination of smartphone technology and PHM technology to provide a software app that can be used to monitor personal health outside a clinical set up and on the go regardless of users' expertise. The question then becomes are there moral issues that could be presented by this combination of processes and procedures? An example here could now be smartphone apps that store and provide location data that could be used for uberveillance and other unwarranted purposes therefore posing an ethical concern. The combination of the smartphone and the app have a potential of using both features of each different level of the technology therefore represent novel ethical concerns. This shows that as more artifacts emerge, new ethical concerns will be realised.

The third level is the application of SPHM apps. The focus at his level is what context is a SPHM app being used, where is the app being used and who is using it (user characteristics) in relation to the inherent features of the app. Is it for home or professional use? The context in which the SPHM app is used will pose different ethical concerns. An example is when an SPHM app is used by people in 2 different cultural systems the ethical concerns that may arise could potentially be different. In one, the dissemination of app data could not pose as many consequences as in another due to differences in strength and establishment of the regulatory system of the country of origin for the app an what is culturally acceptable or not.

Similarly, the aim of SPHM app would potentially determine the ethical concerns that its use is likely to present. In this case an ideological scenario could be apps that are used for activity monitoring whereby their users are subscribed to a social media group to get tips and offers on products that are tailor-made according to the data provided by the user, will have different potential ethical concerns to apps that are used for measuring glucose levels in order to prompt the user to take remedial action such as an insulin injection without passing on information to a third party at that particular moment.

5. CONCLUSION

The literature survey shows that there is limited literature that is specifically directed at ethical concerns that affect SPHM apps however, if these apps are considered in the context of their features, an inference of ethical concerns with similar ubiquitous computing devices could be used to realise ethical concerns that affect SPHM apps. With this in mind, ethical concerns of SPHM apps could be realised through speculation on what sort of ethical concerns could emerge at different levels of the technology's focus. This highlights a need for more research that is specific to

SPHM apps and probably an empirical study of what different stakeholders of the technology think are the existing and potential ethical concerns with SPHM apps.

6. ACKNOWLEDGMENTS

Thanks to Prof. Bernd Stahl and Dr. Catherine Flick for your support towards this paper.

7. REFERENCES

[1] Ackerman, L. 2013. *Mobile Health and Fitness Applications and Information Privacy*. California Consumer Protection Foundation. Privacy Clearing House.

[2] Al Ameen, M. et al. 2012. Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. *Journal of Medical Systems*. 36, 1 (Feb. 2012), 93–101.

[3] Bazeley, P. and Jackson, K. 2013. *Qualitative data analysis with NVivo*. SAGE Publications Ltd.

[4] Boulos, M.N.K. et al. 2011. How smartphones are changing the face of mobile and participatory healthcare: an overview, with example from eCAALYX. *BioMedical Engineering OnLine*. 10, (Apr. 2011), 24.

[5] Brey, P.A.E. 2012. Anticipating ethical issues in emerging IT. *Ethics and Information Technology*. 14, 4 (Dec. 2012), 305–317.

[6] Enck, W. 2011. Defending users against smartphone apps: Techniques and future directions. *Information Systems Security*. Springer. 49–70.

[7] Gasson, M.N. et al. 2011. Normality Mining: Privacy Implications of Behavioral Profiles Drawn From GPS Enabled Mobile Phones. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*. 41, 2 (Mar. 2011), 251–261.

[8] Giota, K.G. and Kleftaras, G. 2014. Mental Health Apps: Innovations, Risks and Ethical Considerations. *E-Health Telecommunication Systems and Networks*. 03, 03 (2014), 19–23.

[9] Hayes, D.F. et al. 2014. Personalized medicine: risk prediction, targeted therapies and mobile health technology. *BMC medicine*. 12, 1 (2014), 37.

[10] HowSmartphonesChangingHealthCare.pdf: 2010. *http://www.chcf.org/~/media/MEDIA%20LIBRARY%20Files/PDF/H/PDF%20HowSmartphonesChangingHealthCare.pdf*. Accessed: 2014-10-20.

[11] Istepanian, R.S.H. et al. 2004. Guest Editorial Introduction to the Special Section on M-Health: Beyond Seamless Mobility and Global Wireless Health-Care Connectivity. *IEEE Transactions on Information Technology in Biomedicine*. 8, 4 (Dec. 2004), 405–414.

[12] Michael, K. and Clarke, R. 2013. Location and tracking of mobile devices: Überveillance stalks the streets. *Computer Law & Security Review*. 29, 3 (Jun. 2013), 216–228.

[13] Michael, M. and Michael, K. 2010. Toward a State of uberveillance. *IEEE Technology and Society Magazine*. 29, 2 (2010), 9–16.

[14] Milani, P. et al. 2014. Mobile Smartphone Applications for Body Position Measurement in Rehabilitation: A Review of Goniometric Tools. *PM&R*. (May 2014).

[15] Milosevic, M. et al. 2011. Applications of Smartphones for Ubiquitous Health Monitoringand Wellbeing Management. *Journal of Information Technology and Applications*. 1, 1 (2011), 7–15.

[16] Mittelstadt, B. et al. 2014. The Ethical Implications of Personal Health Monitoring. *International Journal of Technoethics (IJT)*. 5, 2 (2014), 37–60.

[17] Moor, J.H. 2005. Why We Need Better Ethics for Emerging Technologies. *Ethics and Information Technology*. 7, 3 (Sep. 2005), 111–119.

[18] Orwat, C. et al. 2008. Towards pervasive computing in health care – A literature review. *BMC Medical Informatics and Decision Making*. 8, 1 (Jun. 2008), 26.

[19] Rose, N. 2014. The Human Brain Project: Social and Ethical Challenges. *Neuron*. 82, 6 (Jun. 2014), 1212–1215.

[20] Stahl, B.C. et al. 2014. From computer ethics to responsible research and innovation in ICT. *Information & Management*. 51, 6 (Sep. 2014), 810–818.

[21] Tene, O. and Polonetsky, J. 2013. Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Intellectual Property*. 11, 5 (2013), 239–273.

[22] Thomas, C.M. et al. 2013. Smartphones and computer tablets: Friend or foe? *Journal of Nursing Education and Practice*. 4, 2 (Dec. 2013).

[23] Tran, J. et al. 2012. Smartphone-based glucose monitors and applications in the management of diabetes: an overview of 10 salient "apps" and a novel smartphone-connected blood glucose monitor. *Clinical Diabetes*. 30, 4 (2012), 173–178.

[24] VodafoneGlobalEnterprise-mHealth-Insights-Guide-Evaluating-mHealth-Adoption-Privacy-and-Regulation.pdf: *http://mhealthregulatorycoalition.org/wp-content/uploads/2013/01/VodafoneGlobalEnterprise-mHealth-Insights-Guide-Evaluating-mHealth-Adoption-Privacy-and-Regulation.pdf*. Accessed: 2015-01-07.