The Impact of Gamification on mHealth Fitness Application Privacy Literacy

Trevor Clohessy  
Business Information Systems,  
National University of Ireland, Galway

Grace Kenny  
Business Information Systems,  
Dublin City University

Keywords: mHealth, Privacy Literacy, Gamification, Coping Mechanisms, Fitness Applications

INTRODUCTION:

The use of mobile health (mHealth) applications for incentivizing health behaviour change continues to grow at an unprecedented rate. This growth has been accelerated by recent advancements in ‘smart’ mobile technology such as cloud computing, internet of things, sensors, phones, tablets, wristbands and watches. Physicians and other health care professionals are increasingly advising their patients on the merits of using these applications as health monitoring (e.g. diabetes, heart rate etc.) and health improvement tools (e.g. smoking cessation, weight control etc.). mHealth fitness applications such as Fitbit, Jawbone, Fuelband, and Nike+ have become increasingly popular with an estimated 25 million fitness applications sold in 2015 (GFK, 2015). However, in order for these applications to be truly effective they require the user to be wholly comfortable and transparent with the levels of personal data which are entered into and subsequently generated by these devices. For instance, the majority of these fitness applications monitor heart rate, chart sleep patterns, log exercise, diet and calories, enable social media sharing and compare users to their peers in order to set goals. It is widely agreed that privacy represents a barrier to the continued success of mHealth (Mosa et al. 2012; Whittaker, 2012). However, the importance of privacy contrasts with the current practices of mHealth providers who tend to utilize opaque, lengthy privacy policies and engage in excessive sharing of data with a multitude of third parties, some of whom are not listed in the privacy policy (Privacy Rights ClearingHouse, 2013). Thus, there is an apparent need to investigate the changing role of privacy in the health context.

RESEARCH MOTIVATION:

This study is motivated for several reasons. First, there is currently a dearth of information systems (IS) research pertaining to consumer’s health privacy literacy levels in the context of mHealth fitness applications. This is significant as there is evidence to suggest that these nascent applications may pose
serious privacy concerns (Blenner et al. 2016). Furthermore, in general, consumers do not read the terms and conditions of their privacy policies indicating a current lack of privacy literacy (Steinfeld 2016; Jensen and Potts, 2004). Second, there is a dearth of IS research identifying the specific inhibitors which negatively impact consumers’ willingness to use mHealth fitness applications. This is compounded by the fact that mHealth service providers are struggling to attract new consumers as a result of recent privacy controversies and an overcrowded application market. Finally, while extant research has examined the use of gamification strategies to incentivize the repeated use of fitness applications amongst consumers (e.g. Lister et al. 2016), no research has explored the potential for mHealth service providers to use gamification coping mechanisms as a method for improving consumer’s health privacy literacy levels. In particular, the specific gamified coping mechanisms these organizations could use to navigate through unchartered digital privacy waters is an area which is ripe for further investigation. With this in mind, figure 1 presents a simple research model which depicts the focus of the study. Specifically, this study seeks to answer two interrelated research questions:

RQ1: How does consumers’ comprehension of mHealth privacy literacy impact their willingness to use mHealth fitness applications?

RQ2: How can gamification coping mechanisms be used to increase mHealth privacy literacy and minimize inhibitors which reduce consumers’ willingness to use mHealth applications?

![Research Model](image)
THEORETICAL FOUNDATION:

It is important at the outset to define what is meant by the term privacy. The privacy phenomenon has been studied for centuries across numerous academic disciplines such as Law, Marketing, and Information Systems. Advances in digital technology have led to a surge in information privacy research in recent decades leading to a myriad of conflicting definitions of the concept. Privacy is a multidimensional and polymorphous concept which is studied from a variety of different lenses. As a result, it is argued that it may not be possible to develop a single, comprehensive, unambiguous definition of information privacy (Pavlou, 2011). It is thus imperative to define information privacy within the discipline of the researcher and the context of the study. A widely cited definition in the IS literature defines information privacy as an individual’s desire to have more control over the collection and dissemination of their information (Bélanger and Crossler, 2011). This definition is adapted in this paper and information privacy is defined as an individual’s desire to have greater control over the collection and dissemination of their health information by mHealth application providers.

The existing literature on the relationship between privacy and mHealth adoption is limited. However, prior studies show that privacy concerns can reduce individuals’ intentions to use mHealth applications (Hwang et al. 2012) and perceptions of privacy risk can negatively impact intentions and actual use of wearable health devices (Li et al. 2016). In addition, studies in the Internet context show that individuals may adopt technologies but may falsify the data they disclose due to concern for privacy (Stutzman et al., 2011; Keith et al. 2015). Thus, privacy or individuals’ perception that they cannot control their health data, is an inhibitor facing adoption of mHealth. In line with previous findings, this study posits that perceived risk or fear of negative outcomes from mHealth use, and privacy concerns are likely to reduce individuals’ willingness to use mHealth applications and disclose detailed sensitive data. However, prior research suggests that these inhibitors could be addressed by increasing individuals’ perceived control over their health data and building trust (Dinev et al. 2016). It is thus proposed that individuals’ perception of risk fears and concerns can be addressed and appeased by improving individuals’ mHealth privacy literacy, thereby fostering a sense of trust and enhancing their perception of control over their health data. The concept of privacy literacy is a new concept which “assesses and explains the consumer’s attitude regarding the collection, processing and employment of their personal data” (Veghes
Privacy literacy has not yet been explored in the mHealth context, however it can be argued that improving individuals’ understanding of how mHealth applications collect, process, and use their health data can address concerns that data will be misused and reduce fears regarding possible negative repercussions stemming from such use.

In terms of research question 2, this study will investigate how gamification coping mechanisms can be used to increase mHealth literacy and minimize inhibitors (e.g. perceived lack of control of data, privacy concerns, lack of trust etc.) which negatively impact consumers’ willingness to use mHealth fitness applications. Gamification is rapidly growing in popularity among practitioners, business professionals and academics alike. Leveraging game design elements, gamification is currently being used in non-game contexts to enhance products and services in order to intrinsically motivate customers toward preferred behaviours, enhance end-users’ experiences and increase employees’ incentivization and engagement (Deterding et al. 2011; Blohm and Leimeister, 2013; Seaborn and Fels, 2015). A recent ‘Gamification 2020’ report highlights how gamification, combined with other emerging trends and technologies, will have a significant impact on: innovation, the design of employee performance, the emergence of customer engagement platforms and the gamification of personal development (Gartner, 2014). From an academic perspective, gamification has also received increasing attention in recent years (Huotari and Hamari, 2012; Thiebes et al. 2014; Seaborn and Fels, 2015). This is underlined by gamification’s popularity across academic outlets in terms of journal special issues, conference tracks, special interest groups, workshops, panels and so on. Additionally, the appearance of the terms ‘gamification’ and ‘game elements’ as methods with which to motivate and engage end-users are fast increasing in popularity with regards to academic inquiry (Thiebes et al. 2014; Hamari et al., 2014).

**NEXT STEPS AND CONTRIBUTION**

The research is in its early stages and is currently focused on theory building. The study will harness a three stage sequential mixed methods research design to develop an in-depth multi-perspective understanding of the new mHealth privacy literacy concept (Venkatesh et al. 2013). The first phase will consist of expert interviews comprising mHealth fitness application service providers to understand their current privacy practices and identify the important privacy issues that should be highlighted to users. Combining the judgment of a large number of experts offers a better chance of getting closer to the
‘truth’. It is also easier to understand the intricacies of a phenomena by obtaining the views of the actors that have been immersed within it (Dalkey and Helmer, 1963; Linstone and Turoff, 1975). Phase two will use focus groups comprising a randomized sample of digital native consumers. Focus groups enable IS researchers to gain “a deeper understanding of the topic of interest by providing more background information about the circumstances of the participant’s answers or opinions” (Belanger, 2012). The aim of the focus groups is to ascertain the dominant concerns of participants regarding mHealth applications. The final phase will consist of a series of laboratory-based experiments during which we will use a number of gamified-based scenarios to assess the impact of specific gamification coping mechanisms on developing mHealth fitness privacy literacy and diminishing the negative impacts of privacy related inhibitors.

When completed the research hopes to make a number of contributions. Firstly, from an empirical perspective the research will add to the limited body of literature on the role of privacy in the mHealth context and deepen our understanding by conceptualizing and testing the role of mHealth privacy literacy as a means of addressing privacy and building trust in mHealth technology vendors. The special nature of the health context calls for unique theorizing to understand the role of IS in this context (Agarwal et al. 2010). The study aims to add greatly to the theoretical foundations in this area by building theory for understanding the role of mHealth privacy literacy in increasing willingness to disclose health data. From a practice perspective, gamification has been used successfully by companies such as Nike, Deloitte, Samsung and Cisco. However, it has been estimated by technology consultancy company Gartner that approximately 80% of organisations’ attempts to gamify their service bundles will fail due to inappropriate design and fine-tuning (Gartner, 2014). Additionally, there is a lack of standardized guidelines available for deploying coping mechanisms aimed at gamifying consumer mHealth privacy literacy. Thus, the purpose of this study is to work with mHealth fitness application service providers and consumers in order to build an improved understanding and foster trust to increase mHealth adoption and users’ willingness to disclose detailed personal data. Ultimately, we envisage that our research will have implications for the manner with which mHealth service providers design and incorporate gamified privacy policies in their fitness application service bundles.
REFERENCES:


