Summer 6-27-2016

DOES PRIVACY THREAT MATTER IN MOBILE HEALTH SERVICE? FROM HEALTH BELIEF MODEL PERSPECTIVE

Hui-Mei Hsu
National Kaohsiung Normal University, hmhsu@nknu.edu.tw

DOES PRIVACY THREAT MATTER IN MOBILE HEALTH SERVICE? FROM HEALTH BELIEF MODEL PERSPECTIVE

Hui-Mei, Hsu, Department of Business Management, National Kaohsiung Normal University, Kaohsiung, Taiwan, hmhsu@nknu.edu.tw

Abstract

A lot of mobile health (mHealth) service apps have been launched in the market with advances in technology. When people decide to use these mHealth service apps, they have to provide their personal data or personal health data more or less to the service providers. However, the health data is more sensitive data than general personal data. In addition, the behaviour of using mHealth service apps includes technology use behaviour and health promotion behaviour. Therefore, we employed HBM to be the theory foundation to find out what factors will impact on the intention to upload personal health data via a mHealth service app. Online questionnaires were distributed and 133 valid questionnaires were returned. The results showed the perceived benefits is the only factor to influence an individual intention to upload personal health data. The specific information privacy concerns has no significant effect on the behaviour intention. That means people value the benefits that the mhealth service app can bring more than the threat of privacy they perceived. The construct, disposition to value privacy (DTVP), have strong effects on perceived vulnerability, perceived severity, and specific information privacy concerns. Future studies will be recommended.

Keywords: information privacy concerns, privacy threat, health belief model, mhealth

1 INTRODUCTION

With the great popularity of smartphone, many mobile (Apps) are developed continuously. According to the statistics of smartphone apps by March 2015, the number of app and times of download are 1,205,000/29,000,000,000 for apple ios and 950,000/31,000,000,000 for google android system. Among all app categories, healthcare & Fitness has 4% market share, it is higher than business category (3%) and social networking category (2%)"Mobile Phone App Store Statistics" 2014). The mature of Internet of Things(IOT) technology drives many wearable devices invention such as apple watch and medical machines adding the function of connecting the internet (such as blood glucose monitors) to enter the mobile health (mHealth) market. According to the investigation of research2guidance, 36% mobile app providers entered mHealth market, and the number of mHealth apps grows year by year. The mHealth apps are various, such as fitness, medical condition management, and PHR(personal health record) (see figure 1). The forecast of mHealth market they made will reach US$ 26 billion globally by 2017(Research2guidance 2014).

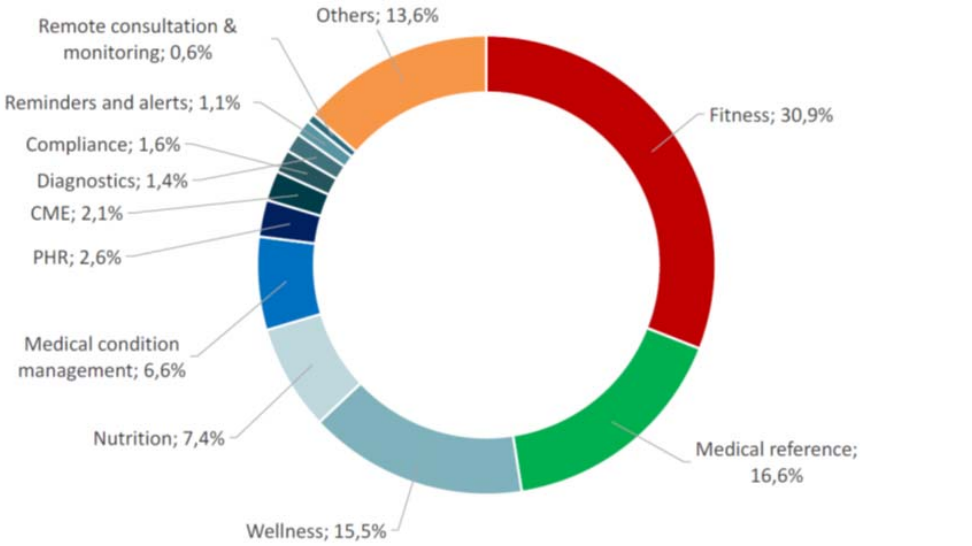


Figure 1. mHealth app category share (Source fromResearch2guidance (2014))

Numerous mHealth apps provide different services. One type is providing health information only (e.g. Best Diet Foods); another type is focused on self-health management, thus, it provide personalized and recording functions (e.g. iBP Blood Pressure); some mHealth service apps provide auto-collecting health data measured by a measurement device (e.g. apple watch) and auto-uploading to servers. Even fewer mHealth service providers proposed a healthcare management service that integrated hospitals, medical device suppliers, and technology of the internet to provide a remote healthcare service to users by professional medical staff (e.g. Blood Glucose Care Project). No matter which service that mentioned above, they are provided through smartphone apps. Therefore, these services are referred to mHealth service apps in this study.

An individual have to provide personal data and health data more or less when he/she uses the mHealth service apps. However, parts of personal health data may be sensitive, such as past disease history, sexual behaviours, family history, or a hereditary disease(s). These data is helpful for medical staff to make an accurate diagnosis or clinical decision. In the light of the sensitivity of health data, the information privacy concerns (IPC) of people on the health data is higher than other personal data (Rohm & Milne 2004), thus, people may provide personal health data reluctantly or selectively (Sankar, Mora, Merz, & Jones 2003). In the circumstances, the way mHealth service app providers treat their users is similar to companies which monitor, collect, access, and even deliver customers'

data for providing customized or personalized services/products to customers(Chellappa & Sin 2005). Thus, customers usually face the privacy dilemmas (or privacy paradox) of providing personal data to enjoy personalized service or providing limited personal data to protect their privacy(Awad & Krishnan 2006; Chellappa & Sin 2005; Dinev & Hart 2006; Norberg, Horne, & Horne 2007; Xu, Luo, Carroll, & Rosson 2011).

Recently, the growth of cloud computing makes people are highly concerned about their privacy, confidentiality, and security. Because people worry that their personal data will be leaked on purpose or incautiously by cloud service providers (Ryan 2011). Nowadays, people and their own smartphone are inseparable, and many mHealth service apps employ a smartphone as a data input device. Therefore, it is worth to notice that if mHealth service app providers take advantage of a smartphone to collect/ monitor users' data/ behaviours. Is it a threat to users' privacy?

Shukla (2014) proceeded a field experiment to discuss personalization privacy paradox in smartphone apps. The results showed that users had a higher process and content gratification for a personalized, privacy-safe application than a personalized, non-privacy-safe application. Comparing to the non-personalized application, users who use a personalized, privacy-safe application displayed higher satisfaction only with content gratification. The results implied a personalized, privacy-safe application provide a personalized service and protect users' privacy can earn their gratification in both content and process. In addition, this study also mentioned the type of information involved whether determine the relationship between privacy concerns and the gratification users obtain from personalized service. For this reason, the adoption of mHealth service apps is an important issue because health data/information are more private and sensitive.

Past research related information privacy concerns were focus on the intention of data providing or e-commerce (Bansal, Zahedi, & Gefen 2010; Dinev, et al. 2006; Dinev & Hart 2006; Eastlick, Lotz, & Warrington 2006; Liao, Liu, & Chen 2011; Malhotra, Kim, & Agarwal 2004; Olivero & Lunt 2004; Phelps, Nowak, & Ferrell 2000; Sheng, Nah, & Siau 2008; Son & Kim 2008) or to discover factors that influence information privacy concerns(Anderson & Agarwal 2011; Bansal, et al. 2010; Dinev & Hart 2006; Liao, et al. 2011; Xu, Dinev, Smith, & Hart 2011). Most previous research findings displayed that an individual who has higher information privacy concern will lower his/her intention to provide personal data (Anderson & Agarwal 2011; Bansal, et al. 2010; Dinev & Hart 2006; Malhotra, et al. 2004; Olivero & Lunt 2004; Sankar, et al. 2003; Sheng, et al. 2008; Son & Kim 2008; Xu, Dinev, et al. 2011; Yawn, Yawn, Geier, Xia, & Jacobsen 1998). In addition, some research discussed information privacy concerns in different environment, such as online IPC (Li, Sarathy, & Xu 2010; Liao, et al. 2011), general IPC (Li, et al. 2010; Liao, et al. 2011; Xu, Luo, et al. 2011), thus, Li (2014b) argued IPC belief will change with the environment, and only IPC belief for specific environment will impact on individual behaviour.

The behaviour of using mHealth service apps includes two dimensions: one is the behaviour of using technology, the other is the health promotion behaviour. Most research related technology use in the past were based on technology acceptance Model (TAM), the theory of reasoned action (TRA), the theory of planned behaviour (TPB). However, these theories are sufficiently comprehensive enough while applying to health promotion behaviours. In the healthcare field, health belief model (HBM) is used to discuss publics' or patients' health behaviour, such as health screen, helmet utilization, or compliance behaviour.

Health Belief Model (HBM) is used to explain or predict an individual health behaviour (Rosenstock 1966). Health belief model (HBM) originated with social psychologists of the department of public health of America in exploring the factors causing thorough failure of people 's acceptance of screening tests for asymptomatic disease or early detection tests (e.g. vaccination, health examination) in the 1950s. In the early stage, HBM focused on the discussion of individual preventive health behaviour. Until 1974, Becker (1974) applied HBM to the behaviours of patients (sick role). Hereafter, researcher started to study patients' compliance behaviours or other health-related behaviours (Becker & Maiman 1975; Becker, Maiman, Kirscht, Haefner, & Drachman 1977). In 1984, Janz and Becker

reviewed a decade of HBM studies and found that the main factor affecting an individual to adopt health behaviour is perceived barrier, and the next one is perceived susceptibility; for the sick role, the results displayed the effect of perceived severity would replace perceived susceptibility(Janz & Becker 1984). The diversity of mHealth service apps makes users with different roles. For example, the users of blood glucose care project should be a sick role; an individual using apple watch to record activities or heart rate may be a preventive health behaviour.

Recently, some researcher employed HBM to study users' secure behaviour in technology-mediated financial transactions or computer security, and the authors argued that HBM is a proper theory to apply to security behaviours of information technology environment (Davinson & Sillence 2014; Ng, Kankanhalli, & Xu 2009). According to the statement of Son and Kim (2008), the one of the main risks of mHealth services is the threat of privacy invasion, thus, information privacy concerns is a manifestation of perceived privacy threat. We regard information privacy concerns as a perceived privacy threat from mHealth service providers and integrated HBM to empirically examine what factors that influence individual intention to upload personal health data via mHealth service apps.

In view of mHealth service apps have both characteristics of technology and healthcare, hence it is proper to study people's behaviour intention basing on HBM. The purposes of this research are to empirically examine the explanation power of HBM, to find out the role of privacy threat play, and to explore what factors will impact on an individual intention to upload personal data via mHealth service apps.

2 LITERATURE REVIEW

2.1 Health Belief Model

Health Belief Model (HBM) is proposed by four researchers, Hochbaum, Leventhal, Kegeles and Rosenstock, and used to explain and predict an individual health behaviour (Rosenstock 1966). HBM includes several constructs—perceived susceptibility, perceived severity, perceived threat, perceived benefit, perceived barriers, and cue to action. Additionally, self-efficacy in social cognitive theory is also an important factor. Rosenstock, Strecher, and Becker (1988) pointed out that HBM was applied to the discussion of PHR in an early stage. Since PHR is usually doing once or ends in the short term (e.g. vaccinations or health screening tests), therefore self-efficacy was not under consideration. Later, while HBM was applied to the discussion of SBR, the behaviour change of chronic patients is long-term instead, such as life style, diets, exercises, taking medicines..., thus self-efficacy became a critical factor in HBM.

2.2 Information Privacy Concerns

Privacy concern is the concern of protection against privacy invasion, unwarranted communication, and misuse of personal information (Bansal, et al. 2010; Smith, Milberg, & Burke 1996). Information privacy concern is the concern about the control of information, security of information exchange, and whether their information will be used appropriately(Bansal, et al. 2010). While the internet grows vigorously, online merchants might collect, store, use, and deliver customers' personal information without customers' permission, thus people raise their information privacy concern and worry about misuse of their personal information by online merchants (Chellappa & Sin 2005). Recently, the growing cloud services have encountered the same issue that the public concerns their privacy and security would be infringed because cloud service providers might disclosure their personal information on purpose or unintentionally (Ryan 2011).

Li (2011) reviewed 82 research that studied information privacy concerns in electronic commerce setting. He induced antecedents and consequences of information privacy concerns and proposed an integrated framework. He mentioned that personal factors (such as demographics, personalities, personal knowledge and experience), social psychology factors (e.g. self-efficacy), social-relational

factors (e.g. social norm), organizational and task environmental factors (enterprise reputation, social presence), macro-environmental factor (culture value, governmental regulatory structures), and information contingencies (e.g. information type, information sensitivities) are antecedents of general concerns for information privacy (CFIP) or specific CFIP, the consequence constructs of specific CFIP included trust belief, perceived privacy risks, behaviour intention, and actual behaviours (e.g. refuse to provide personal data, remove information, negative word of mouth, complain). Through the integrated framework contributed by Li, we could have a more comprehensive understand about CFIP.

In addition, Li (2014b) reviewed several previous literature and found inconsistency of the relationship between CFIP and consumers' behaviour among those research results. Li argued one of the factors that caused inconsistency may be the different measurements of information privacy concerns. The information privacy concerns of previous studies focused on different targets, such as specific websites, particular suppliers, general online environment, or specific health information. Therefore, he proposed a multi-level concept and concluded three levels of information privacy concerns; those are disposition to privacy, online privacy concerns, and website privacy concerns.

2.3 Hypothesis development

According to HBM theory, we employed perceived susceptibility, perceived severity, perceived threat, perceived benefits, perceived barriers, and self-efficacy constructs in our study. Considering the characteristics of health service apps, people may connect to the internet and upload their personal health data. Thus, they may put themselves in a risky environment. However, the perceived threat was a focus on the threat of specific disease, consider the context of this research, the threat construct was replaced with information privacy concerns (threat of privacy invasion), and the perceived susceptibility was replaced with perceived vulnerability since the target behaviour is not focused on a specific disease. In this study, we will base on HBM to examine the relationship among privacy threat, perceived benefits/barriers, and upload health data.

The personal disposition to value privacy (DTVP) is a personality attribute or an individual's general tendency to maintain personal boundaries of information protection (Xu, Dinev, et al. 2011). Previous studies showed DTVP has significant impacts on privacy concerns in several circumstances, such as EC, healthcare, social networking (Li 2014a, 2014b; Xu, Dinev, et al. 2011). Thus, we proposed the first hypothesis as follows:

H_1: DTVP has a positive effect on information privacy concerns.

Perceived susceptibility and perceived severity are important antecedents of perceived threat in past HBM studies(Janz & Becker 1984). Ross, Ross, Rahman, and Cataldo (2010) use HBM theory to discuss bicycler's attitude to a bicycle helmet, and they replace perceived susceptibility with perceived vulnerability. From the perspective of protection motivation theory (PMT), researchers found that perceived vulnerability had a positive influence on perceived threat of computer virus (Lee, Larose, & Rifon 2008). In social network site, people who perceived higher severity have higher information privacy concerns (Mohamed & Ahmad 2012). Since DTVP is a personality attribute or an individual's general tendency, trait theories suggest that individual characteristics may have a potential impact on a person's privacy beliefs (Smith, Dinev, & Xu 2011). Thus, we assume boldly that individual characteristics will affect his/her perceptions. According to the results of previous research, the H_2 -H_5 were proposed as follows:

H_2: DTVP has a positive effect on perceived vulnerability.

H_3: DTVP has a positive effect on perceived severity.

H_4: Perceived vulnerability has a positive effect on information privacy concerns.

H_5: Perceived severity has a positive effect on information privacy concerns.

Self-efficacy was regarded as an important factor that influence people to proceed the health behaviour (Rosenstock, et al. 1988). In MIS filed, self-efficacy was a critical antecedent of IS use or continuous

use behaviour (Compeau & Higgins 1995; Hsu, Chiu, & Ju 2004). Past studied found people with higher self-efficacy understand the privacy operations of websites more than people with lower self-efficacy (Rifon, LaRose, & Choi 2005). Therefore, people who have higher self-efficacy will understand the benefits and barriers of the target behaviour more completely. Other research found self-efficacy has a positive relationship with information privacy concerns (Chai, Bagchi-Sen, Morrell, Rao, & Upadhyaya 2009; Mohamed & Ahmad 2012). The following hypotheses were proposed:

H_6: Self-efficacy has positive effects on information privacy concerns.

H_7: Self-efficacy has a positive effect on perceived benefits.

H_8: Self-efficacy has a negative effect on perceived barriers.

H_9: Self-efficacy has a positive effect on intention to upload personal health data.

Many previous studies displayed the negative relationship between Information privacy concerns and information disclosure(Anderson & Agarwal 2011; Bansal, et al. 2010; Dinev & Hart 2006; Malhotra, et al. 2004; Olivero & Lunt 2004; Sankar, et al. 2003; Sheng, et al. 2008; Son & Kim 2008; Xu, Dinev, et al. 2011; Yawn, et al. 1998). Undoubtedly, we will propose the same hypothesis. Perceived benefits and perceived barriers were proved that they were strong predictors of health behaviour(Carpenter 2010). In information privacy research, Li (2014a) confirmed the perceived benefits had a positive impact on behaviour intention. Thus, we proposed hypotheses as follows:

H_{10}: Information privacy concerns has a negative effect on intention to upload personal health data.

H_{11}: Perceived benefits has a positive effect on intention to upload personal health data.

H_{12}: perceived barriers has a negative effect on intention to upload personal health data.

3 RESEACH METHOD

3.1 Data Collection

Due to the diversity of mHealth service apps those provide different health services, users will confront different contingencies. A few services only need users to record daily diets information, some of the services request users to measure their daily health data (such as blood pressure value) and upload to the app's platform. Therefore, we employed one health service app to be the target app that could make each participant confront the same app while answering the questionnaire. The health app we chose is "Little Health Secretary", which is provided by Pfizer Inc. (see figure 2). We made an introduction video to illustrate the functions of "Little Health Secretary" and the data they collect from the users. All participators should watch the introduction video of Little Health Secretary app first, then they are allowed to answer the questionnaire. Participators were recruited from social network sites, or bulletin board system (BBS) sites.

Figure 2 The screen shot of Little Health Secretary app

3.2 Constructs and Measurements

Except for those items measuring perceived benefits and perceived barriers, all measurement items of each construct were derived from prior research. Since items adapted from past studies were in English originally, we translated them into traditional Chinese first and then made minor modifications in order to fit them into our research context. All items were scored on a 7-point Likert scale, anchored from 1 (strongly disagree) to 7 (strongly agree).

4 RESULTS

4.1 Description Statistics

One hundred and thirty-three valid questionnaires were collected. The demographics analysis showed female respondents was the majority (60.9%). The age 20-29 was the largest share (66.2 %), the next one was age 30-39 (25.5%). Near half respondents (48.9%) think their health status was better than publics, 36.8% respondents were equal to publics, and 14.3 % were worse.

4.2 Measurement Model Analysis

The PLS-SEM was used in this study. The values of Cronbach's α and composite reliability were higher than 0.8. Thus, the reliability of measurements is not an issue. The AVE of each construct was higher than 0.5, that achieves the Fornell & Larcker's rule (1981) of convergent validity. the square root of AVE of each construct was larger than the correlation between the specific construct and any other constructs, and the loading of each measurement item was highest on its theoretical construct, therefore the discriminant validity was confirmed(Chin 1998). The details was displayed in table 1.

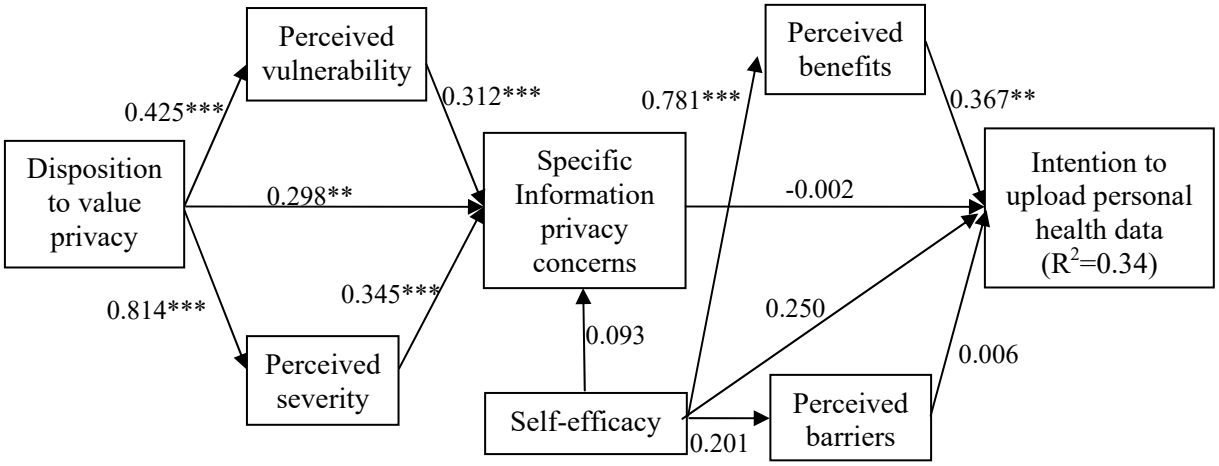
Table 1 The Results of Reliability and Validity

Construct	AVE	Cronbach's α	Composite Reliability	Correlation Matrix							
				DTVP	PB	PBA	PC	PS	PV	SE	UI
DTVP	0.795	0.871	0.921	0.892							
PB	0.855	0.958	0.967	0.342	0.925						
PBA	0.659	0.887	0.906	0.243	0.017	0.812					
PC	0.578	0.919	0.932	0.750	0.219	0.377	0.760				
PS	0.855	0.943	0.959	0.814	0.210	0.198	0.735	0.924			
PV	0.830	0.932	0.951	0.425	0.039	0.335	0.584	0.377	0.911		
SE	0.779	0.959	0.966	0.419	0.781	0.201	0.383	0.323	0.172	0.882	
UI	0.904	0.948	0.966	0.314	0.561	0.062	0.176	0.164	0.086	0.537	0.951

note:
1. DTVP: Disposition to value privacy, PB: Perceived benefits, PBA: Perceived barriers, PC: Specific Information privacy concerns, PS: Perceived severity, PV: Perceived vulnerability, SE: Self-efficacy UI: Intention to upload personal health data
2. Square root of the AVE was displayed on the diagonal of correlation matrix

4.3 Path Model Analysis

According to the rules of thumb for the bootstrap routine, we bootstrapped 5000 samples(Hair Jr, Hult, Ringle, & Sarstedt 2013). The result of path model test was showed in figure 3. As we can see, the personal disposition to value privacy has a significant impact on perceived vulnerability, perceived severity, and specific information privacy concerns; perceived vulnerability and perceived severity have significant impacts on specific information privacy concerns. However, the specific information privacy concerns has no significant effect on the intention to upload personal health data. This is different from previous research. Only the perceived benefits construct has a significant effect on the intention to upload personal health data. The self-efficacy has an impact on the perceived benefits only. The R^2 of the intention to upload personal health data is 0.34.



** p<0.05, ** p<0.01, *** p<0.001*

Figure 3 The results of path model analysis

5 CONCLUSION

The result of the relationship between specific information privacy concerns and the intention to upload personal health data is unexpected. The results showed the perceived benefits is the only factor to influence an individual intention to upload personal health data. The possible reasons might be the characteristics of mhealth app we chose or the self-reported bias. The data that people can upload while using "Little Health Secretary" includes body weight, blood pressure, pulse(heartbeat rate), blood glucose, allergy history, and the name of medicine. However, the app does not require users to log in or input personal information (such as name, age, gender, ID...). Therefore, users may ignore the privacy threat and still intent to upload their health data for using mhealth service. This study only considers one app situation, we recommend more various health service apps can be studied in further research to understand information privacy issues comprehensively. The majority of samples in this study are young people. In general, the health condition of young people is well. Most of them don't have the experience to measure blood pressure/glucose every day and record them. Thus, the self-reported bias might occur in this study.

The results showed the personal disposition to value privacy (DTVP) have strong effects on perceived vulnerability, perceived severity, and specific information privacy concerns. It illustrated that individuals who have higher DTVP feel more vulnerability, severity, and the threat of privacy invasion. Thus, DTVP is a strong predictor for the individual perception of privacy invasion and privacy beliefs.

Finally, only one construct, perceived benefits, has a significant impact on the intention to upload personal health data. Self-efficacy, perceived barriers, and specific information privacy concerns didn't show the influences on it. The results displayed that people value the benefits that the mhealth service app can bring more than the threat of privacy they perceived. Thus, health service app provider should enhance the benefits they can contribute.

References

Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. Information Systems Research, 22(3), 469-490.

Awad, N. F., & Krishnan, M. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. MIS Quarterly, 13-28.
Bansal, G., Zahedi, F. M., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decision support systems, 49(2), 138-150.
Becker, M. H. (1974). The Health Belief Model and Sick Role Behavior. Health Education & Behavior, 2(4), 409-419.
Becker, M. H., & Maiman, L. A. (1975). Sociobehavioral determinants of compliance with health and medical care recommendations. Medical care, 13(1), 10-24.
Becker, M. H., Maiman, L. A., Kirscht, J. P., Haefner, D. P., & Drachman, R. H. (1977). The Health Belief Model and prediction of dietary compliance: a field experiment. Journal of Health and Social Behavior, 18(4), 348-366.
Carpenter, C. J. (2010). A meta-analysis of the effectiveness of health belief model variables in predicting behavior. Health communication, 25(8), 661-669.
Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H., & Upadhyaya, S. J. (2009). Internet and online information privacy: An exploratory study of preteens and early teens. Professional Communication, IEEE Transactions on, 52(2), 167-182.
Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. Information Technology and Management, 6(2), 181-202.
Chin, W. W. (1998). The partial least squares approach to structural equation modeling. Modern methods for business research, 295(2), 295-336.
Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. MIS Quarterly, 19(2), 189-211.
Davinson, N., & Sillence, E. (2014). Using the health belief model to explore users' perceptions of 'being safe and secure'in the world of technology mediated financial transactions. International Journal of Human-Computer Studies, 72(2), 154-168.
Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce–a study of Italy and the United States. European Journal of Information Systems, 15(4), 389-402.
Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information Systems Research, 17(1), 61-80.
Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. Journal of Business Research, 59(8), 877-886.
Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. Journal of marketing research, 382-388.
Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2013). *A primer on partial least squares structural equation modeling (PLS-SEM)*: Sage Publications.
Hsu, M. H., Chiu, C. M., & Ju, T. L. (2004). Determinants of continued use of the WWW: an integration of two theoretical models. Industrial management & data systems, 104(9), 766-775.
Janz, N. K., & Becker, M. H. (1984). The health belief model: A decade later. Health Education & Behavior, 11(1), 1-47.
Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. Behaviour & Information Technology, 27(5), 445-454.
Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. Journal of Computer Information Systems, 51(1), 62-71.
Li, Y. (2011). Empirical studies on online information privacy concerns: literature review and an integrative framework. Communications of the Association for Information Systems, 28(1), 453-496.
Li, Y. (2014a). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. Decision support systems, 57, 343-354.

Li, Y. (2014b). A multi-level model of individual information privacy beliefs. Electronic Commerce Research and Applications, 13(1), 32-44.
Liao, C., Liu, C. C., & Chen, K. (2011). Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model. Electronic Commerce Research and Applications, 10(6), 702-715.
Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information Systems Research, 15(4), 336-355.
Mobile Phone App Store Statistics. (2014). Retrieved Dec, 10, 2014, from http://www.statisticbrain.com/mobile-phone-app-store-statistics/
Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. Computers in Human Behavior, 28(6), 2366-2375.
Ng, B.-Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. Decision support systems, 46(4), 815-825.
Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of Consumer Affairs, 41(1), 100-126.
Olivero, N., & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. Journal of Economic Psychology, 25(2), 243-262.
Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. Journal of Public Policy & Marketing, 27-41.
Research2guidance. (2014). mHealth App Developer Economics 2014. Retrieved Nov, 30, 2014, from http://mhealtheconomics.com/mhealth-developer-economics-report/
Rifon, N. J., LaRose, R., & Choi, S. (2005). Your privacy is sealed: effects of web privacy seals on trust and personal disclosures. Journal of Consumer Affairs, 39(2), 339-362.
Rosenstock, I. M. (1966). Why people use health services. The Milbank Memorial Fund Quarterly, 43(3), 94-127.
Rosenstock, I. M., Strecher, V. J., & Becker, M. H. (1988). Social learning theory and the health belief model. Health Education & Behavior, 15(2), 175-183.
Ross, T. P., Ross, L. T., Rahman, A., & Cataldo, S. (2010). The bicycle helmet attitudes scale: using the health belief model to predict helmet use among undergraduates. Journal of American College Health, 59(1), 29-36.
Ryan, M. D. (2011). Cloud computing privacy concerns on our doorstep. Communications of the ACM, 54(1), 36-38.
Sankar, P., Mora, S., Merz, J. F., & Jones, N. L. (2003). Patient perspectives of medical confidentiality. Journal of general internal medicine, 18(8), 659-669.
Sheng, H., Nah, F. F. H., & Siau, K. (2008). An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns. Journal of the Association for Information Systems, 9(6), 344-376.
Shukla, P. (2014). The impact of organizational efforts on consumer concerns in an online context. Information & Management, 51(1), 113-119.
Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. MIS Quarterly, 35(4), 989-1016.
Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. MIS Quarterly, 167-196.
Son, J.-Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. MIS Quarterly, 32(3), 503-529.
Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. Journal of the Association for Information Systems, 12(12), 798-824.

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. Decision support systems, 51(1), 42-52.

Yawn, B. P., Yawn, R., Geier, G., Xia, Z., & Jacobsen, S. (1998). The impact of requiring patient authorization for use of data in medical records research. The Journal of family practice, 47(5), 361.